FAST®

FW300R

300M无线宽带路由器

详细配置指南

1910070049 Rev: 2.0.0

声明

Copyright © 2011 深圳市友佳联科技有限公司

版权所有，保留所有权利

未经深圳市友佳联科技有限公司明确书面许可，任何单位或个人不得擅自仿制、复制、誊抄或转译本书部分或全部内容。不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

FAST®为深圳市友佳联科技有限公司注册商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

联系方式

网址：www.fastcom.com.cn

技术支持热线：400-8830-660

技术支持 E-mail：fae@fastcom.com.cn

目 录

第 1 章　产品概述 1

1.1　产品简介 1
1.2　主要特性 1

第 2 章　硬件描述 3

2.1　面板布置 3
2.1.1　前面板 3
2.1.2　后面板 4
2.2　复位 5
2.3　系统需求 5
2.4　安装环境 5
2.5　硬件安装步骤 5

第 3 章　快速安装指南 7

3.1　建立正确的网络设置 7
3.2　快速安装指南 8

第 4 章　配置指南 12

4.1　启动和登录 12
4.2　运行状态 12
4.3　设置向导 14
4.4　WPS一键安全设定 14
4.5　网络参数 21
4.5.1　LAN口设置 21
4.5.2　WAN口设置 22
4.5.3　MAC地址克隆 29
4.6　无线设置 29
4.6.1　基本设置 30
4.6.2　无线安全设置 30
4.6.3　无线MAC地址过滤 34
4.6.4　无线高级设置 36
4.6.5　主机状态 37
4.7　DHCP服务器 37
4.7.1　DHCP服务 38
4.7.2　客户端列表 39
4.7.3　静态地址分配 39
4.8　转发规则 40
4.8.1　虚拟服务器 40
4.8.2　特殊应用程序 42
4.8.3　DMZ主机 43
4.8.4　UPnP设置 44

4.9 安全设置 45
4.9.1 防火墙设置 45
4.9.2 IP地址过滤 46
4.9.3 域名过滤 47
4.9.4 MAC地址过滤 49
4.9.5 远端WEB管理 50
4.9.6 高级安全设置 52
4.10 路由功能 53
4.10.1 静态路由表 53
4.11 IP带宽控制 54
4.12 IP与MAC绑定 55
4.12.1 静态ARP绑定设置 56
4.12.2 ARP映射表 57
4.13 动态DNS 57
4.14 系统工具 58
4.14.1 时间设置 59
4.14.2 诊断工具 59
4.14.3 软件升级 62
4.14.4 恢复出厂设置 63
4.14.5 备份和载入配置 64
4.14.6 重启路由器 66
4.14.7 修改登录口令 66
4.14.8 系统日志 66
4.14.9 流量统计 67
附录A FAQ 68
附录B IE浏览器设置 72
附录C 规格参数 74

第1章 产品概述

1.1 产品简介

迅捷 FW300R 11N 无线宽带路由器是专为满足小型企业、办公室和家庭办公室的无线上网需要而设计，它功能实用、性能优越、易于管理。

迅捷 FW300R 11N 无线宽带路由器基于 IEEE 802.11n 标准，它能扩展无线网络范围，提供最高达 300Mbps 的稳定传输，同时兼容 IEEE 802.11b 和 IEEE 802.11g 标准。传输速率的自适应性提高了本路由器与其他网络设备进行互操作的能力。大范围的无线覆盖空间为您提供了自由轻松的网络环境。稳定的数据传输以及带宽供给为您的网上冲浪、MP3 下载、网络电话、文件共享、网络游戏等网络服务提供了强大的技术保证，实现无忧上网。

迅捷 FW300R 11N 无线宽带路由器提供多重安全防护措施，可以有效保护用户的无线上网安全。支持 SSID 广播控制，有效防止 SSID 广播泄密；支持 64/128/152 位 WEP 无线数据加密，可以保证数据在无线网络传输中的安全。

迅捷 FW300R 11N 无线宽带路由器还提供多方面的管理功能，可以对 DHCP、DMZ 主机、虚拟服务器等进行管理；能够组建内部局域网，允许多台计算机共享一条单独宽带线路和 ISP 账号，并提供自动或按时连通和断开网络连接功能，节省用户上网费用；支持访问控制，可以有效控制内网用户的上网权限。

迅捷 FW300R 11N 无线宽带路由器安装和配置简单，采用全中文的配置界面，每步操作都配有详细的帮助说明。特有的快速配置向导更能帮您轻松快速地实现网络连接。为了充分利用该款路由器的各项功能，请仔细阅读该详细配置指南。

提示:

在本手册中,

- 所提到的路由器，如无特别说明，系指FW300R 11N无线宽带路由器，下面简称为FW300R。
- 用“→”符号说明在WEB界面上的操作引导，其方法是点击菜单、选项、按钮等。
- 路由器配置界面的菜单或按钮名采用“宋体+加粗”字表示，其它选项名或操作项等用“”表示。
- 图片界面都配有相关参数，这些参数主要是为您正确配置产品参数提供参考。实际产品的配置界面并没有提供，您可以根据实际需要设置这些参数。

1.2 主要特性

- 提供一个 10/100M 以太网(WAN)接口，可接 xDSL Modem/Cable Modem/ Ethernet
- 内部集成四口交换机，提供四个 10/100M 以太网(LAN)接口
- 支持最高达 300Mbps 的传输速率，具备速率自适应功能，可以自动调整无线传输速率
- 支持 64/128/152 位 WEP 加密，WPA/WPA2、WPA-PSK/WPA2-PSK 等加密与安全机制，可以保证数据在无线网络传输中的安全
- 支持 11b only、11g only、11n only、11bg mixed 和 11bgn mixed 等多种无线模式
- 支持 SSID 广播控制，有效防止 SSID 广播泄密

- 内置网络地址转换(NAT)功能，支持虚拟服务器、特殊应用程序和 DMZ 主机
- 内建 DHCP 服务器，同时可进行静态地址分配
- 支持 VPN 穿透
- 支持通用即插即用(UPnP)，符合 UPnP 标准的数据可顺利通过
- 内置防火墙功能
- 支持动态 DNS 功能，能够为动态 IP 地址提供域名服务
- 内置静态路由功能，可以根据需要构建特殊网络拓扑
- 支持软件升级，可以免费获得路由器的最新软件
- 可以根据上网动作，自动或按时连通和断开网络连接
- 支持远程和 Web 管理，全中文配置界面
- 支持 WPS 一键安全设定

第2章　硬件描述

2.1 面板布置

2.1.1 前面板

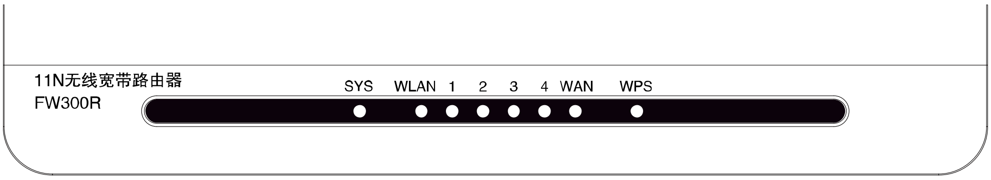


图 2-1 FW300R 前面板示意图

指示灯:

指示灯	说明	描述
SYS	系统状态指示灯	常灭—系统存在故障 常亮—系统初始化故障 闪烁—系统正常
WLAN	无线状态指示灯	常灭－没有启用无线功能 常亮－已经启用无线功能 闪烁－正在进行无线数据传输
1/2/3/4	局域网状态指示灯	常灭—端口没有连接设备 常亮—端口已正常连接设备 闪烁—端口正在传输数据
WAN	广域网状态指示灯	常灭—端口没有连接设备 常亮—端口已正常连接设备 闪烁—端口正在传输数据
WPS	一键安全设定指示灯	慢闪—正在进行安全连接，持续约 2 分钟 慢闪转为常亮—安全连接成功，常亮持续约 5 分钟 慢闪转为快闪—安全连接失败

☞ 注意:

安全连接成功后，WPS 指示灯的常亮状态约持续 5 分钟后会自动熄灭，此种状态仍然属于正常连接状态。

2.1.2 后面板

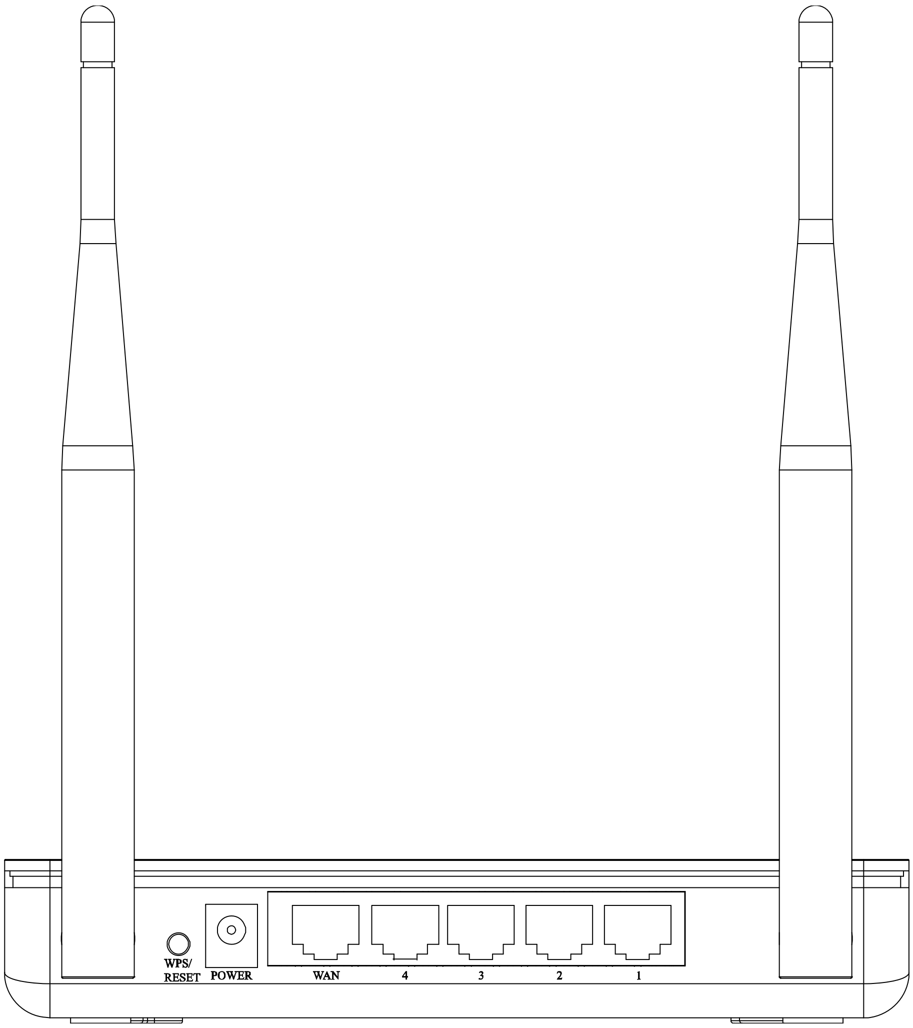


图 2-2 FW300R 后面板示意图

1) **WPS/RESET**：WPS 快速安全设置和 RESET 复位功能的复用按钮。当按住该按钮的时间小于 5 秒，松开按钮时即触发 WPS 功能，用来与具备 WPS 或 QSS 功能的网络设备快速建立安全连接。当按住该按钮的时间长于 5 秒，则直接触发硬件复位功能，用于将设备恢复到出厂默认设置。

2) **POWER**：电源插孔，用来连接电源，为路由器供电。

☞ 注意:

请使用原装电源，如果使用不匹配的电源，可能会导致路由器损坏。

3) **WAN**：广域网端口插孔(RJ45)。该端口用来连接以太网电缆或 xDSL Modem/Cable Modem。

4) **1/2/3/4**：局域网端口插孔(RJ45)。该端口用来连接局域网中的集线器、交换机或安装了网卡的计算机。

5) **天线**：用于无线数据的收发。

2.2 复位

如果要将路由器恢复到出厂默认设置，请在路由器通电的情况下，按住后面板上标识为 WPS/RESET 的按钮，持续 5 秒钟以上，保持按压的同时观察 SYS 灯，当 SYS 灯由缓慢闪烁变为快速闪烁状态时，表示路由器已成功恢复出厂设置，此时松开该按钮，路由器将重启。

☞ 注意:

复位后路由器的所有配置参数将全部被清除，需要对路由器重新进行配置。

2.3 系统需求

- 宽带 Internet 服务(接入方式为以太网电缆接入或通过 xDSL/Cable Modem 接入)
- 具有 RJ45 口的调制解调器(直接使用以太网电缆接入时不需要此设备)
- 每台 PC 的以太网连接设备(无线网卡或有线网卡及网线)
- 支持 TCP/IP 协议的操作系统
- Web 浏览器，如 Microsoft Internet Explorer、Mozilla Firefox、Apple Safari 等

2.4 安装环境

该路由器安装时应该遵循以下原则:

- 将路由器水平放置。
- 尽量远离发热器件，保持通风。
- 不要将路由器置于太脏或潮湿的地方。
- 使用匹配的额定电源适配器。
- 雷雨天气请将设备电源及所有连线拆除，以防雷击。

☞ 注意:

环境因素对传输距离有影响，详细介绍见附录A。

2.5 硬件安装步骤

在安装路由器前，我们希望您已经能够利用您的宽带服务在单台计算机上成功上网。如果您单台计算机上宽带网有问题，请先和您的网络服务商（ISP）联系解决问题。当您成功地利用单台计算机上网后，请遵循以下步骤安装您的路由器。切记安装时拔除电源插头，保持双手干燥。

1. 建立局域网连接

用一根网线连接路由器的LAN口和局域网中的集线器或交换机，如图 2-3所示。您也可以用一根网线将路由器与您的计算机网卡直接相连。

2. 建立广域网连接

用网线连接路由器和xDSL/Cable Modem或以太网，如图 2-3所示。

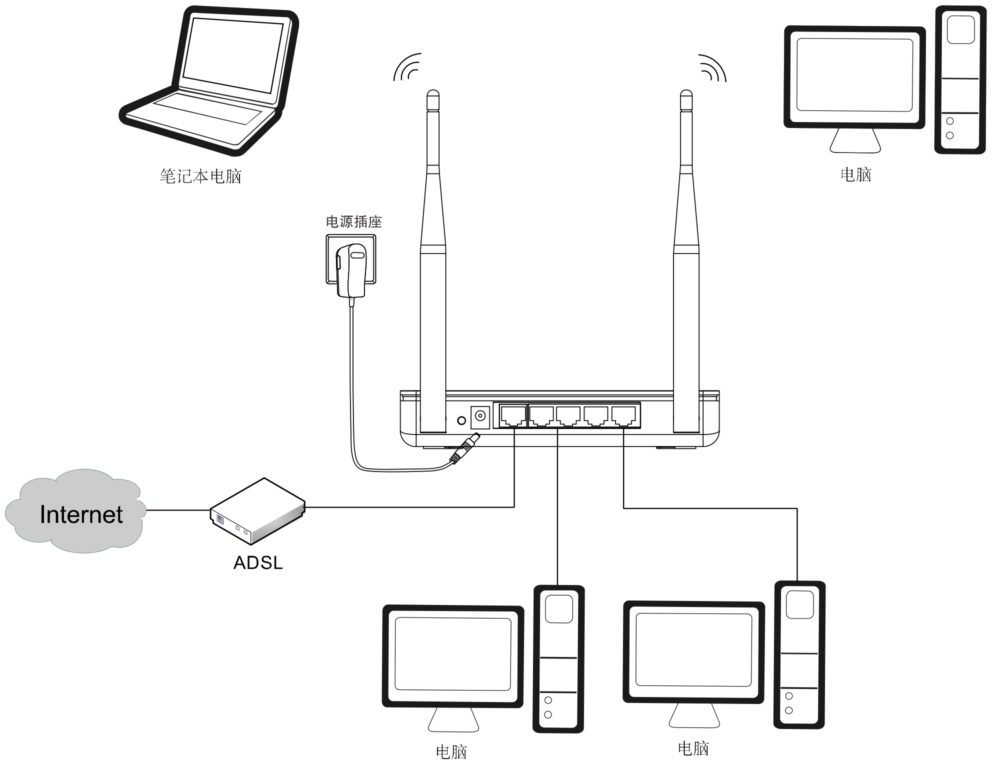


图 2-3 FW300R 硬件安装示意图

3. 连接电源

将电源连接好，路由器将自行启动。

第3章　　快速安装指南

要正确使用路由器，您必须合理配置网络。下面以 Windows XP 为例，讲述具体配置过程。如果只进行基本配置，您只需阅读本章内容；如果要进行高级配置，请继续阅读第四章内容。

3.1　建立正确的网络设置

路由器默认 IP 地址是 192.168.1.1，默认子网掩码是 255.255.255.0。这些值可以根据您的实际需要而改变，但在配置指南中将按默认值说明。

首先请将您的计算机接到路由器的局域网端口，接下来为您的计算机设置 IP 地址。

打开**本地连接－属性－Internet 协议（TCP/IP）**，在**常规**选项卡设置您计算机的 TCP/IP 协议为“自动获取 IP 地址”和“自动获得 DNS 服务器地址”。这样路由器内置 DHCP 服务器将自动为您的计算机设置 IP 地址。

注意:

Windows 98或更早版本的操作系统，以上设置可能需要重启您的计算机。

在设置好 TCP/IP 协议后，您可以使用 Ping 命令检查您的计算机和路由器之间是否连通。下面的例子为一个在 Windows XP 环境中，执行 Ping 命令，操作步骤如下:

点击**开始－运行**，在随后出现的运行窗口输入“cmd”命令，回车或点击**确认**进入下图所示界面。

最后在该界面中输入命令 Ping 192.168.1.1，其结果显示如下。

如果屏幕显示为:

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

这说明您的计算机已与路由器成功建立连接。如果屏幕显示为:

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

这说明设备还未安装好，您可以按照下列顺序检查:

1)　硬件连接是否正确?

提示:

路由器面板上对应局域网端口的 Link/Act 指示灯和您计算机上的网卡灯必须亮。

2) 您的计算机的 TCP/IP 设置是否正确?

提示:

如果路由器的IP地址为192.168.1.1，那么您的计算机IP地址必须为192.168. 1.X（X是2~254之间的任意整数）。

3.2 快速安装指南

本产品提供基于 WEB 浏览器的配置工具，您可以在任何基于 Windows，Macintosh 或 UNIX 平台的 WEB 浏览器（如 Microsoft Internet Explorer、Mozilla Firefox、Apple Safari 等）中使用该配置工具配置您的路由器。

激活浏览器，选择**工具**－**Internet 选项**－**连接**－**局域网设置**，去掉为 **LAN 使用代理服务器**选项或者点击**高级**按钮，在新弹出的窗口**代理服务器设置**中，将路由器的 IP 地址添加到**例外**栏里。接着在浏览器的地址栏里输入路由器的 IP 地址：http://192.168.1.1。

连接建立起来后，您将会看到下图所示登录界面。您需要以系统管理员的身份登录，即在该登录界面输入用户名和密码（用户名和密码的出厂设置均为 **admin**），然后单击确定按钮。

图 3-1 登录窗口

如果用户名和密码正确，浏览器将显示管理员模式的画面，并会弹出一个如图 3-2的设置向导页面（如果没有自动弹出的话，可以单击管理员模式画面左边**设置向导**菜单将它激活）。

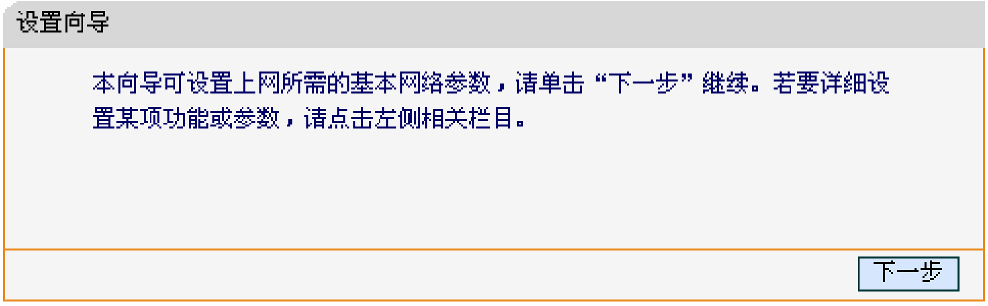


图 3-2 设置向导

单击**下一步**，进入上网方式选择画面。

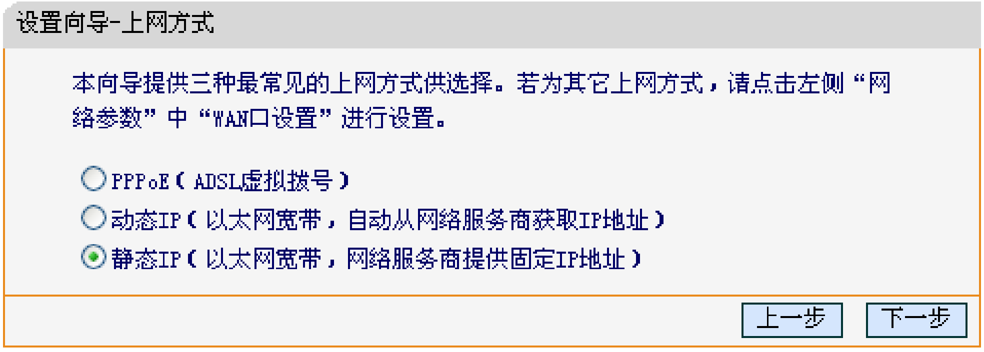


图 3-3 设置向导—上网方式

以上画面显示了最常用的几种上网方式，您可以根据自身情况进行选择，然后单击**下一步**填写上网所需的基本网络参数。

1. PPPoE（ADSL 虚拟拨号）

如果您的上网方式为 PPPoE，即 ADSL 虚拟拨号方式，则您需要填写以下内容：

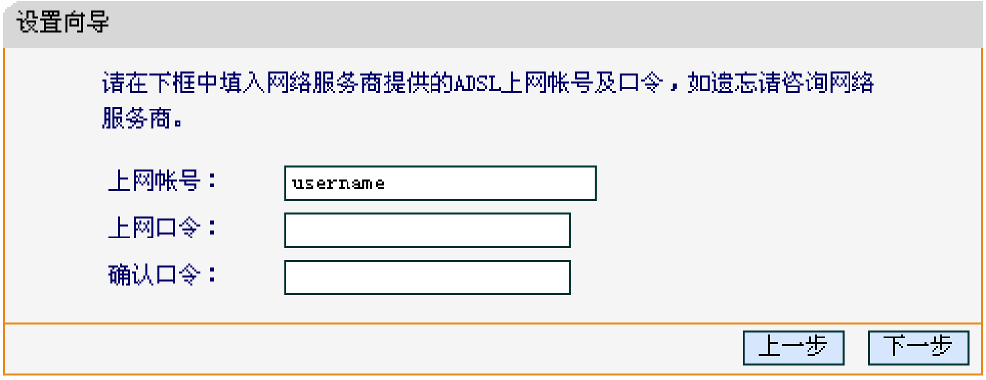


图 3-4 上网方式—PPPoE

- **上网帐号**：填入 ISP 为您指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。
- **上网口令**：填入 ISP 为您指定的 ADSL 上网口令，不清楚可以向 ISP 询问。

2. 动态 IP（以太网宽带，自动从网络服务商获取 IP 地址）

如果您的上网方式为动态 IP，即您可以自动从网络服务商获取 IP 地址，则您不需要填写任何内容即可直接上网。

3. 静态 IP（以太网宽带，网络服务商提供固定 IP 地址）

如果您的上网方式为静态 IP，即您拥有网络服务商提供的固定 IP 地址，则您需要填写以下内容：

图 3-5 上网方式—静态 IP

- **IP 地址**：本路由器对广域网的 IP 地址，即 ISP 提供给您的 IP 地址，不清楚可以向 ISP 询问。
- **子网掩码**：本路由器对广域网的子网掩码，即 ISP 提供给您的子网掩码，一般为 255.255.255.0。
- **网关**：填入 ISP 提供给您的网关，不清楚可以向 ISP 询问。
- **DNS 服务器**：填入 ISP 提供给您的 DNS 服务器地址，不清楚可以向 ISP 询问。
- **备用 DNS 服务器**：可选项，如果 ISP 提供给您了两个 DNS 服务器地址，则您可以把另一个 DNS 服务器地址的 IP 地址填于此处。

设置完成后，单击**下一步**，您将看到图 3-6所示的基本无线网络参数设置页面。

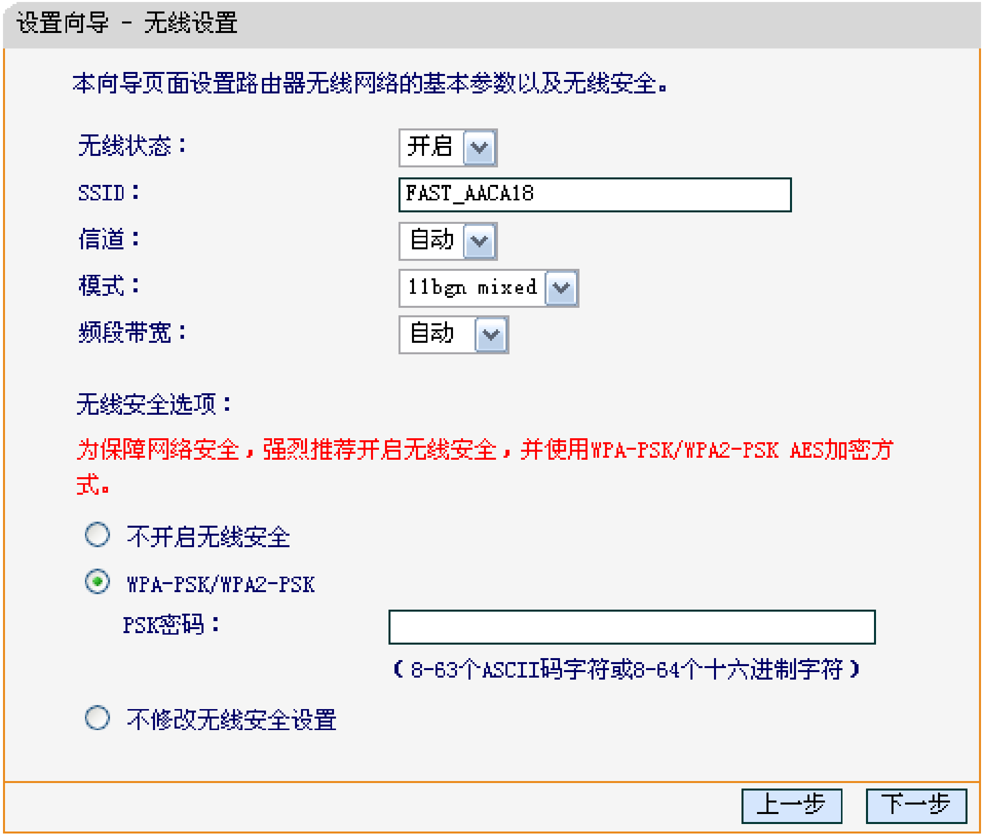


图 3-6 设置向导—无线设置

- **无线状态**：开启或者关闭路由器的无线功能。
- **SSID**：设置任意一个字符串来标明您的无线网络。

- **信道**：设置您路由器的无线信号频段，推荐您使用 1、6、11 频段。
- **模式**：设置您路由器的无线工作模式，推荐您使用 11bgn mixed 模式。
- **频段带宽**：设置无线数据传输时所占用的信道宽度，可选项有：20M、40M 和自动。
- **最大发送速率**：设置您路由器无线网络的最大发送速率。
- **关闭无线安全**：关闭无线安全功能，即您路由器的无线网络不加密。
- **WPA-PSK/WPA2-PSK**：您路由器无线网络的加密方式，如果选择了该项，请在 **PSK 密码**中输入您想要设置的密码，密码要求为 64 个十六进制字符或 8-63 个 ASCII 码字符。
- **不修改无线安全设置**：选择该项，则无线安全选项中将保持您上次设置的参数。如果您从未更改过无线安全设置，则选择该项后，将保持出厂默认设置**关闭无线安全**。

☞ 注意：

以上提到的信道带宽设置仅针对支持 IEEE 802.11n 协议的网络设备，对于不支持 IEEE 802.11n 协议的设备，此设置不生效。

设置完成后，单击**下一步**，如果您更改了无线设置，将弹出图 3-7所示的设置向导完成界面，单击**重启**使无线设置生效。如果您没有更改无线设置，将弹出图 3-8所示的设置向导完成界面，单击**完成**结束设置向导。

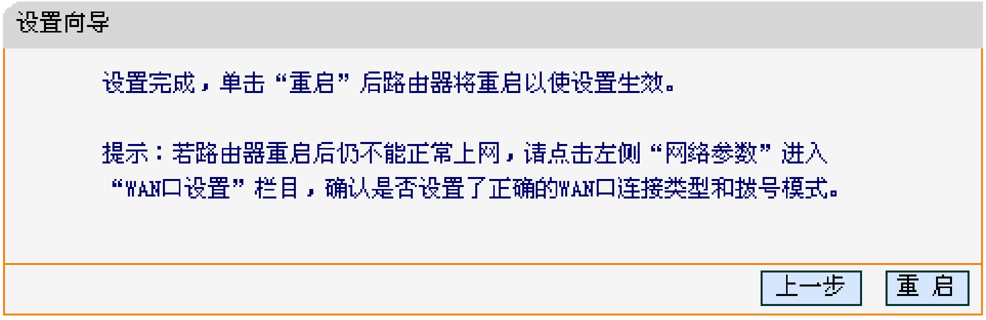


图 3-7 设置完成—重启使设置生效

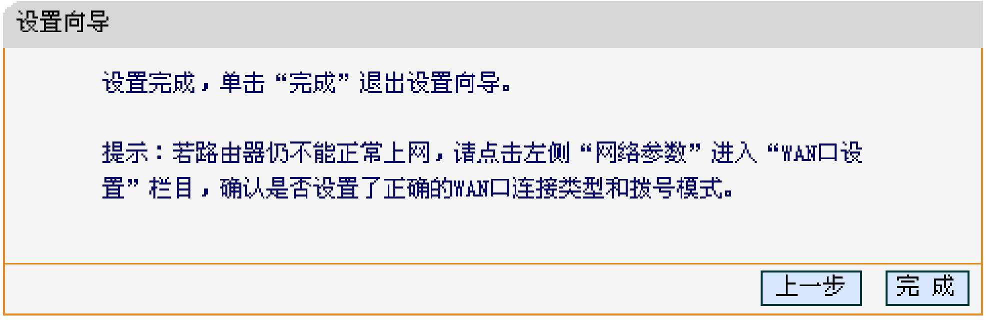


图 3-8 设置完成—结束设置向导

第4章　　配置指南

4.1 启动和登录

启动路由器并成功登录路由器管理页面后，浏览器会显示管理员模式的界面，如图 4-1。

在左侧菜单栏中，共有如下几个菜单：**运行状态**、**设置向导**、**WPS 一键安全设定**、**网络参数**、**无线设置**、**DHCP 服务器**、**转发规则**、**安全设置**、**路由功能**、**IP 带宽控制**、**IP 与 MAC 绑定**、**动态 DNS** 和**系统工具**。单击某个菜单项，您即可进行相应的功能设置。下面将详细讲解各个菜单的功能。

图 4-1　启动和登录

4.2 运行状态

选择菜单**运行状态**，您可以查看路由器当前的状态信息，包括LAN口状态、无线状态、WAN口状态和WAN口流量统计信息，如图 4-2。

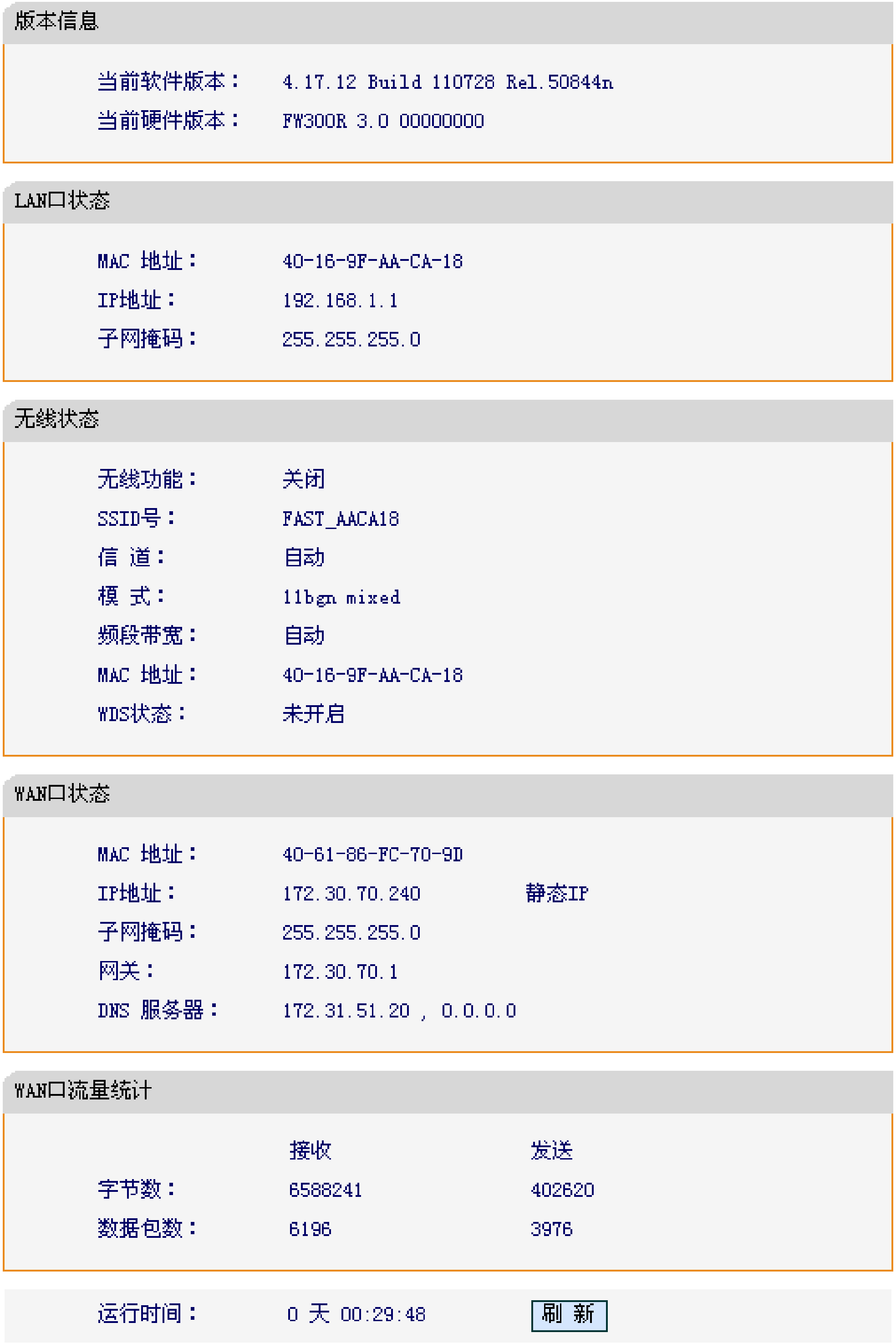


图 4-2 运行状态

- 版本信息：此处显示路由器当前的软硬件版本号。
- LAN口状态：此处显示路由器当前LAN口的MAC地址、IP地址和子网掩码。
- 无线状态：此处显示路由器当前的无线设置状态，包括SSID、频段和频段带宽信息。
- WAN口状态：此处显示路由器当前WAN口的MAC地址、IP地址、子网掩码、网关和DNS服务器地址。
- WAN口流量统计：此处显示当前WAN口接收和发送的数据流量信息。

☞ 注意:

在IP地址右侧会显示用户的上网方式(动态IP/静态IP/PPPoE/L2TP/PPTP/DHCP+)。当用户的上网方式为PPPoE，并且用户已经连接上Internet时，此处将会显示用户的上网时间和断线按钮，单击此按钮可以进行即时的断线操作；如果用户尚未连接Internet时，此处将会显示连接按钮，单击此按钮可以进行即时的连接操作。

4.3 设置向导

请参考**3.2**快速安装指南部分。

4.4 WPS一键安全设定

选择菜单**WPS一键安全设定**，您可以在图 4-3界面中进行快速无线安全设置。

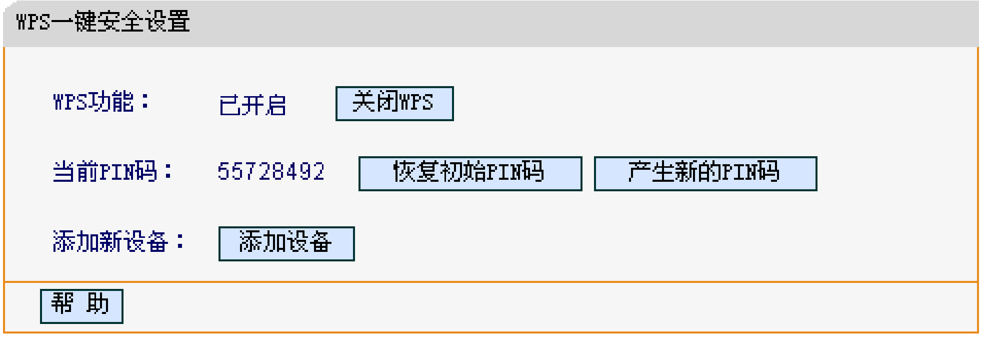


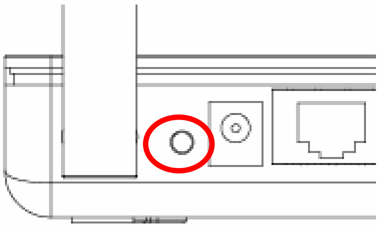
图 4-3 WPS 一键安全设定

- WPS功能：WPS一键安全设定，您可以使用该功能快速建立与无线网卡之间的无线连接。默认状态为开启。
- 当前PIN码：PIN码即个人识别码，用于标识一件无线产品。PIN码可以更改，如果目前使用的PIN码与他人重复，可以点击**产生新的PIN码**，也可以点击**恢复初始PIN码**返回到最初PIN码值。
- 添加新设备：点击添加设备进入添加新设备界面，在此您可以通过手动配置路由器，添加要与其进行连接的无线设备。

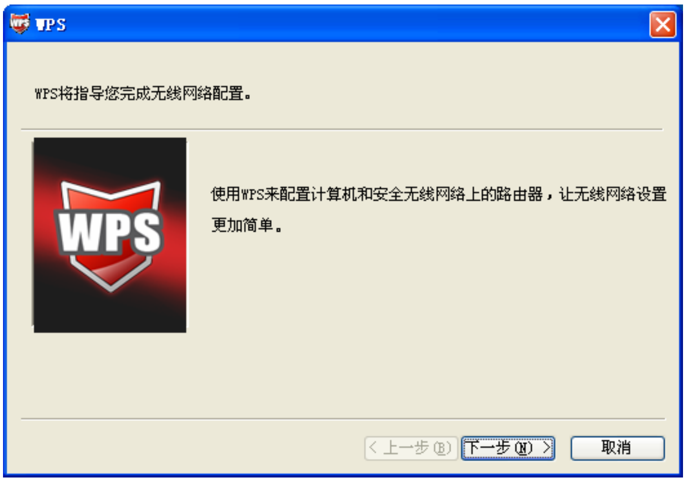
WPS 一键安全设定能够快速建立与无线网卡之间的安全连接。如果您现在拥有支持 WPS 的无线网卡，您可以通过下面任意一种方法快速组建安全的无线网络：

方法一：

1. 按下路由器面板上的WPS一键安全设定按钮。

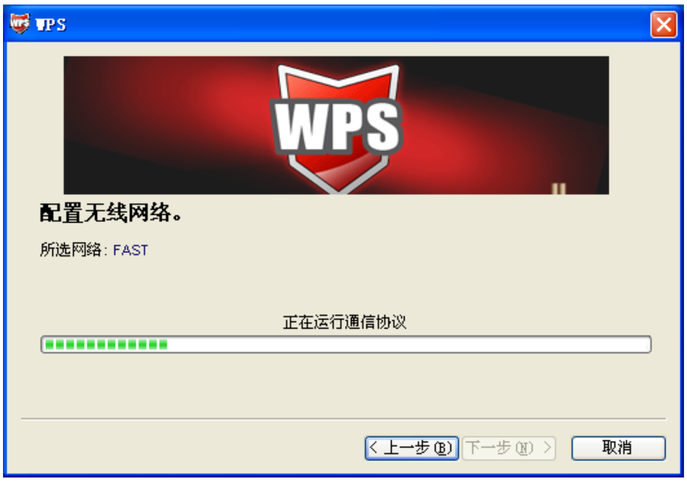


2. 进入网卡WPS软件配置界面，单击下一步。



3. 在随后出现的界面中选择第一项，单击下一步。

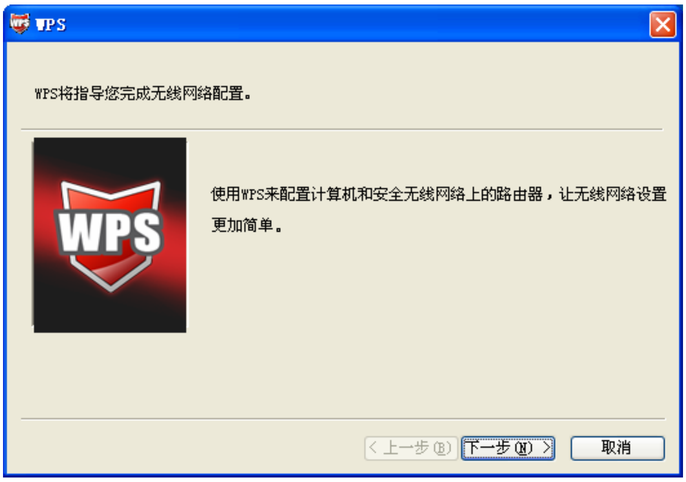
4. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。



5. 出现下图所示界面则表示快速安全连接配置成功，单击**完成**结束。

方法二:

1. 进入网卡WPS软件配置界面，单击下一步。



2. 在随后出现的界面中选择最后一项，并在下面的方框中输入路由器底部标贴上的 8 位 PIN 码，单击下一步。

3. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。

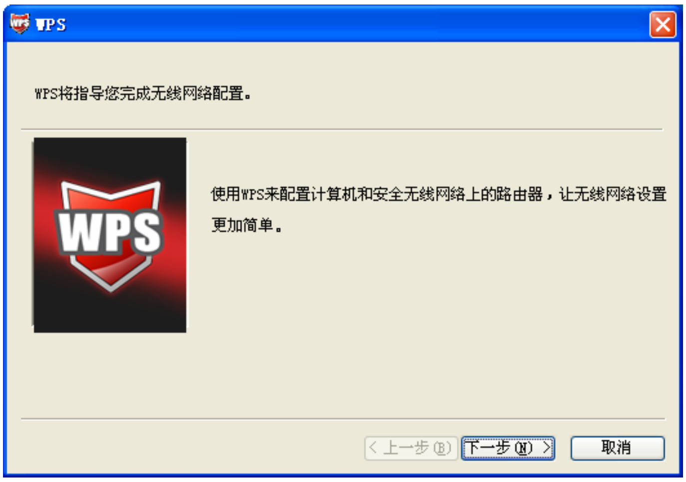
4. 出现下图所示界面则表示快速安全连接配置成功，单击**完成**结束。

方法三:

1. 进入本路由器管理界面，在 “**WPS 一键安全设定**” 界面中选择**添加设备**。

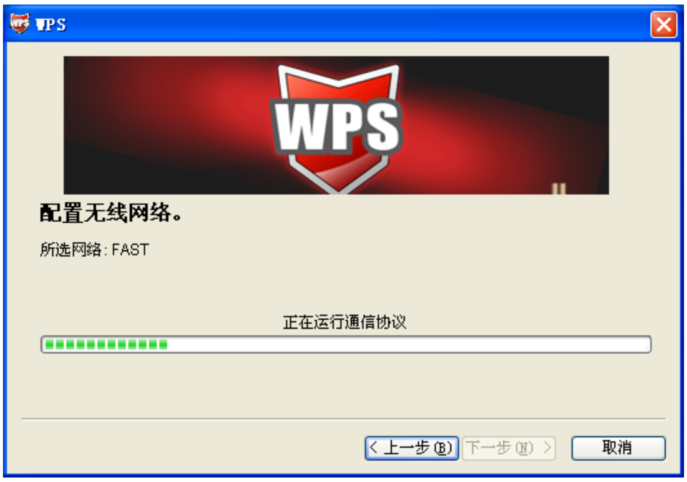
2. 在随后出现的界面中选择**按下新设备上的按钮**，然后点击**连接**按钮。

3. 进入网卡WPS软件配置界面，单击下一步。



4. 在随后出现的界面中选择第一项，单击**下一步**。

5. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。

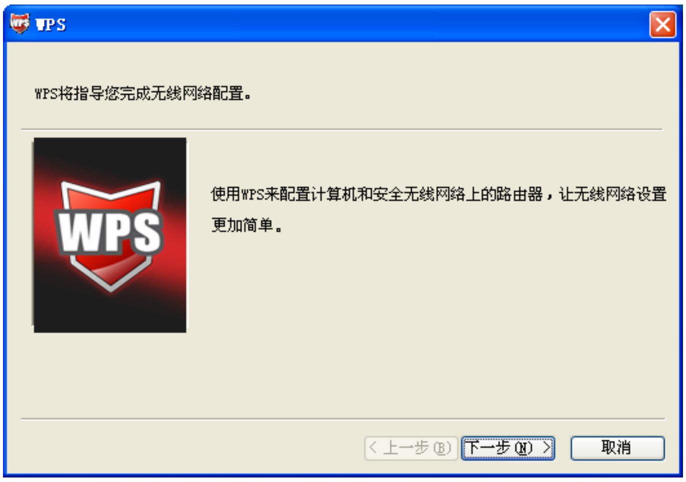


6. 出现下图所示界面则表示网卡端快速安全连接配置成功，单击**完成**结束。

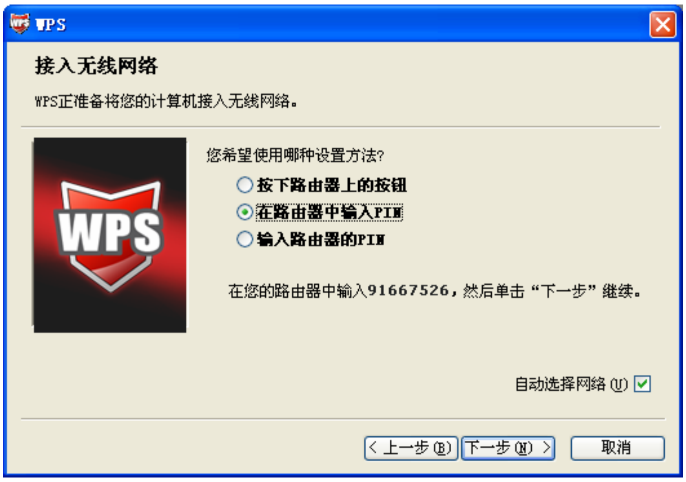
7. 此时路由器端显示添加设备成功。

方法四:

1. 进入网卡WPS软件配置界面，单击下一步。



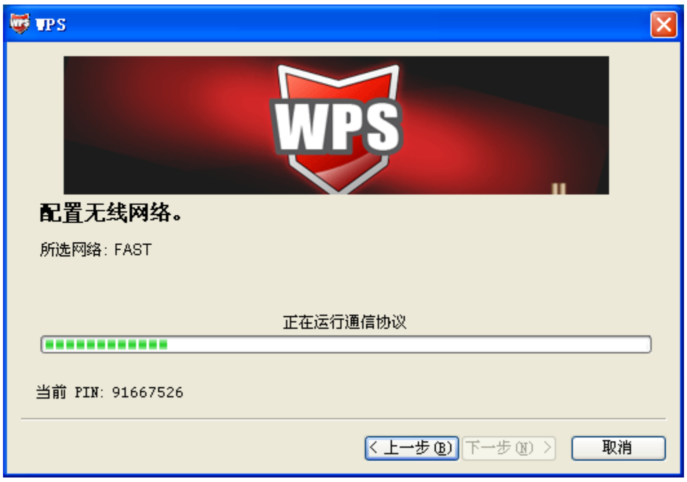
2. 在随后出现的界面中选择第二项，记录粗体显示的8位数字，这便是网卡的PIN码。然后单击下一步。



3. 进入本路由器管理界面，在“**WPS 一键安全设定**”界面中选择**添加设备**。

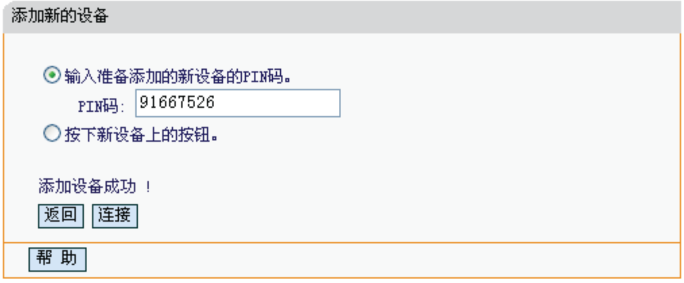
4. 在随后出现的界面中选择**输入准备添加的新设备的 PIN 码**，在下方的 PIN 码框中输入在第 2 步记录的 8 位网卡 PIN 码，然后点击**连接**按钮。

5. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。



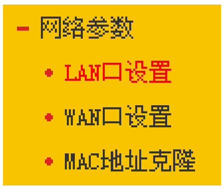
6. 出现下图所示界面则表示网卡端快速安全连接配置成功，单击**完成**结束。

7. 此时路由器端显示添加设备成功。



4.5 网络参数

选择菜单**网络参数**，您可以看到：



单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.5.1 LAN口设置

选择菜单**网络参数→LAN口设置**，您可以在图 4-4界面中配置LAN接口的网络参数。如果需要，可以更改LAN接口IP地址以配合实际网络环境的需要。

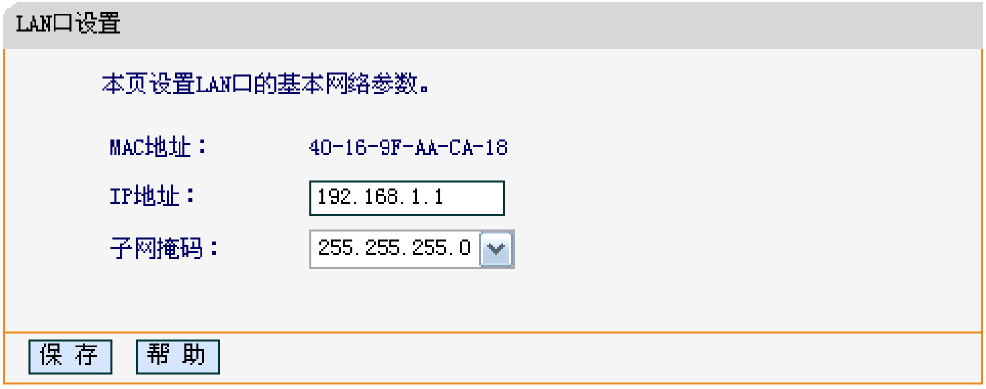


图 4-4 LAN 口设置

- MAC地址：本路由器对局域网的MAC地址，用来标识局域网，不可更改。
- IP地址：本路由器对局域网的IP地址。该IP地址出厂默认值为192.168.1.1，您可以根据需要改变它。
- 子网掩码：本路由器对局域网的子网掩码。您可以根据实际的网络状态输入不同的子网掩码。

完成更改后，点击**保存**按钮以使现有设置生效。

☞ 注意:

1. 如果改变了本地IP地址，您必须用新的IP地址才能登录路由器的WEB管理界面，并且局域网中所有计算机的默认网关必须设置为该IP地址才能正常上网。
2. 局域网中所有计算机的子网掩码必须与此处子网掩码设置相同。

4.5.2 WAN口设置

选择菜单**网络参数→WAN 口设置**，您可以在随后出现的界面中配置 WAN 口的网络参数。

WAN是广域网(Wide Area Network)的缩写。在WAN设置中全部IP信息都是公有IP地址，可以在互联网上访问。本路由器一共提供5种上网方式：动态IP、静态IP、PPPoE、L2TP和PPTP。具体配置时，请首先选择您所需要的WAN口连接类型，即上网方式。如果您不清楚您的上网方式，请咨询您的ISP（网络服务提供商）。本路由器默认上网方式为动态IP。

1. 动态 IP

选择**动态IP**，路由器将从ISP自动获取IP地址。当ISP未给您提供任何IP网络参数时，请选择这种连接方式。如图 4-5。

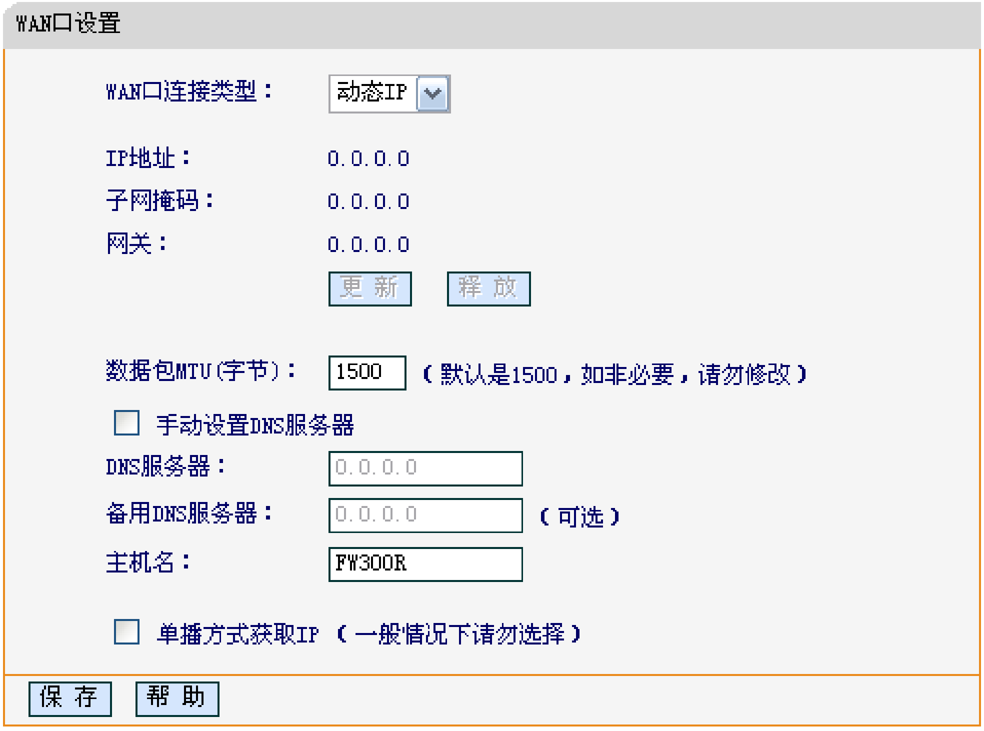


图 4-5 WAN 口设置-动态 IP

- 更新：单击**更新**按钮，路由器将从ISP的DHCP服务器动态得到IP地址、子网掩码、网关以及DNS服务器，并在界面中显示出来。
- 释放：单击**释放**按钮，路由器将发送DHCP释放请求给ISP的DHCP服务器，释放IP地址、子网掩码、网关以及DNS服务器设置。
- 数据包MTU：MTU全称为最大数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。
- DNS服务器、备用DNS服务器：该处显示从ISP处自动获得的DNS服务器地址。若选择**手动设置DNS服务器**，则您可以在此处手动设置DNS服务器和备用DNS服务器(至少设置一个)，连接时，路由器将优先使用手动设置的DNS服务器。
- 单播方式获取IP：少数ISP的DHCP服务器不支持广播请求方式，如果您在网络连接正常的情况下无法获取IP地址，请选择此项。

完成更改后，点击**保存**按钮。

2. 静态 IP

当ISP给您提供了所有WAN IP信息时，请选择**静态IP**，并在图 4-6界面中输入IP地址、子网掩码、网关和DNS地址(一个或多个)。具体设置时，若不清楚，请咨询ISP。如图 4-6。

图 4-6 WAN 口设置-静态 IP

- IP地址：本路由器对广域网的IP地址。请填入ISP提供的公共IP地址，必须设置。
- 子网掩码：本路由器对广域网的子网掩码。请填入ISP提供的子网掩码。根据不同的网络类型子网掩码不同，一般为255.255.255.0(C类)。
- 网关：请填入ISP提供给您的网关。它是连接的ISP的IP地址。
- 数据包MTU：MTU全称为数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。
- DNS服务器、备用DNS服务器：ISP一般至少会提供一个DNS(域名服务器)地址，若提供了两个DNS地址则将其中一个填入“备用DNS服务器”栏。

完成更改后，点击**保存**按钮。

3. PPPoE

如果ISP给您提供的是**PPPoE**(以太网上的点到点连接)，ISP会给您提供上网账号和上网口令。具体设置时，若不清楚，请咨询ISP。如图 4-7。

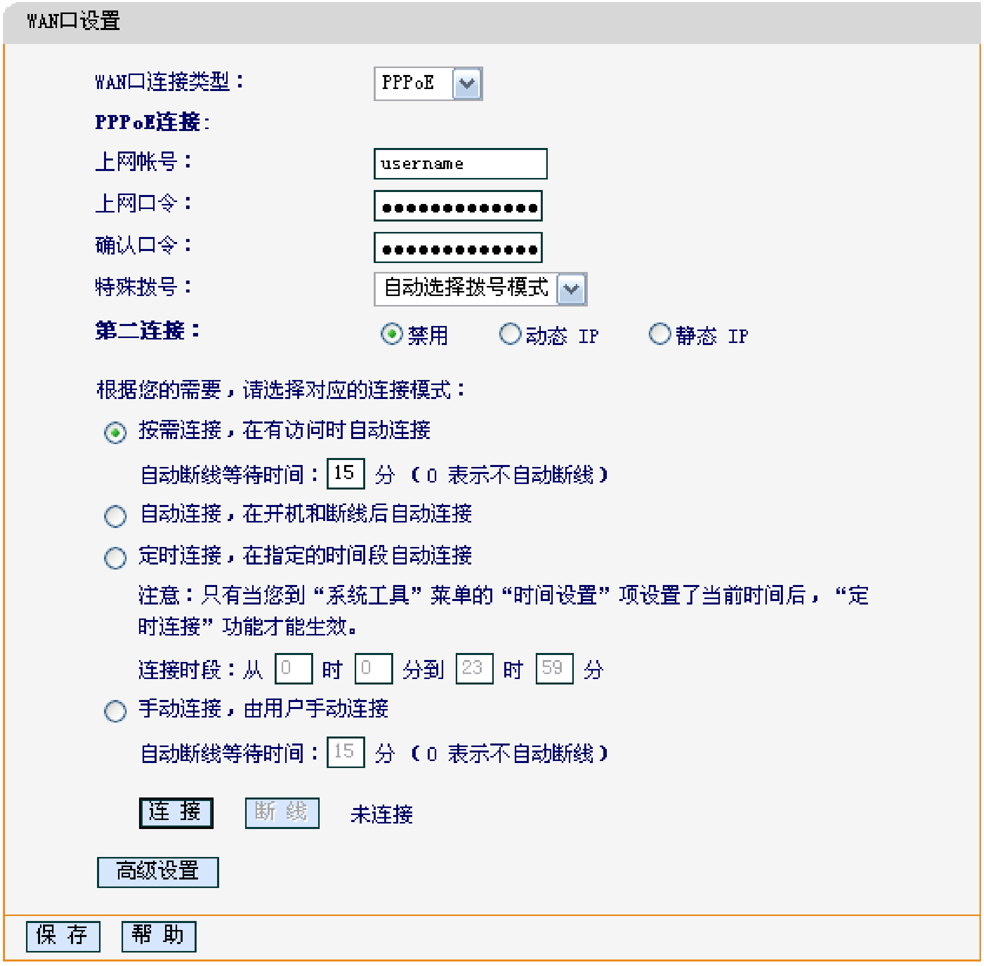


图 4-7 WAN 口设置-PPPoE

- 上网账号、上网口令：请正确填入ISP提供的上网账号和口令，必须填写。
- 第二连接：如果您的ISP额外提供了以动态IP或静态IP的方式连接到局域性网络的连接，那么您可以相应地选择“动态IP”或“静态IP”来启动这个连接。
- 按需连接：若选择**按需连接**模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，可以选择该项连接方式，有效节省上网费用。
- 自动断线等待时间：如果自动断线等待时间T不等于0(默认时间为15分钟)，则在检测到连续T分钟内没有网络访问流量时自动断开网络连接，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。
- 自动连接：若选择**自动连接**模式，则在开机后系统自动进行连接。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(10秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。
- 定时连接：若选择**定时连接**模式，则系统会在连接时段的开始时刻进行网络连接，在指定的终止时刻断开网络连接。选择此连接模式，可以有效控制内网用户的上网时间。
- 手动连接：选择该项，开机后需要用户手动才能进行拨号连接，若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按使用时间进行交费，可以选择该项连接方式。
- 连接/断线：单击此按钮，可进行即时的连接/断线操作。

若需要进一步设置，可以点击**高级设置**按钮，在图4-8界面中进行高级设置。

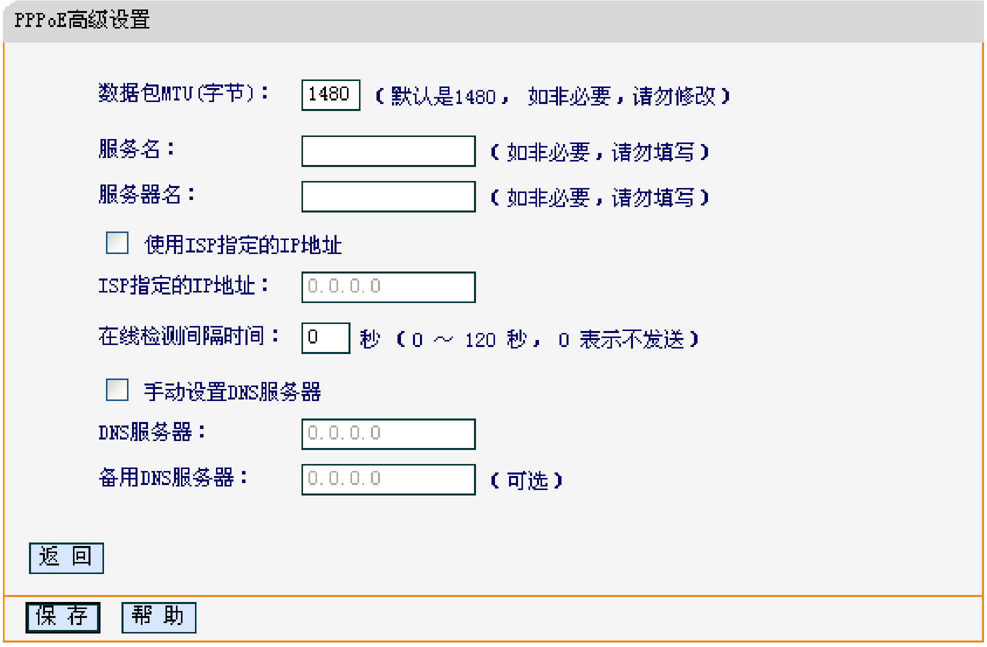


图 4-8 WAN 口设置-PPPoE-高级设置

- 数据包MTU：填入网络数据包的MTU值，缺省为1480，如非特别需要，一般不要更改。
- 服务名、服务器名称：如果不是ISP特别要求，请不要填写这两项。
- 使用ISP指定IP地址：该项仅适用于静态PPPoE。如果您的ISP提供上网账号和口令时，亦提供了IP地址，请选中此选择框，并输入PPPoE连接的静态IP地址。
- 在线检测间隔时间：设置该值后，路由器将根据指定的时间间隔发送检测信号，以检测服务器是否在线。如果该值为0，则表示不发送检测信号。
- DNS服务器、备用DNS服务器：该处显示从ISP处自动获得的DNS服务器地址。若选择**手动设置DNS服务器**，则您可以在此处手动设置DNS服务器和备用DNS服务器(至少设置一个)，连接时，路由器将优先使用手动设置的DNS服务器。

完成更改后，点击**保存**按钮。

4. L2TP

如果ISP给您提供的是L2TP，ISP会给您提供上网账号和上网口令。具体设置时，若不清楚，请咨询ISP。见图 4-9。

图 4-9 WAN 口设置-L2TP

- 上网账号、上网口令：请正确填入ISP提供的上网账号和口令，必须填写。
- 连接/断线：单击此按钮，可进行即时的连接/断线操作。
- 数据包MTU：填入网络数据包的MTU值，缺省为1460，如非特别需要，一般不要更改。
- 按需连接：若选择**按需连接**模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，可以选择该项连接方式，有效节省上网费用。
- 自动连接：若选择**自动连接**模式，则在开机后系统自动进行连接。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(30秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。
- 手动连接：选择该项，开机后需要用户手动才能进行拨号连接，若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按使用时间进行交费，可以选择该项连接方式。

完成更改后，点击**保存**按钮。

5. PPTP

如果ISP给您提供的是PPTP，ISP会给您提供上网账号和上网口令。具体设置时，若不清楚，请咨询ISP。见图 4-10。

图 4-10 WAN 口设置-PPTP

- 上网账号、上网口令：请正确填入ISP提供的上网账号和口令，必须填写。
- 连接/断线：单击此按钮，可进行即时的连接/断线操作。
- 数据包MTU：填入网络数据包的MTU值，缺省为1420，如非特别需要，一般不要更改。
- 按需连接：若选择**按需连接**模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，可以选择该项连接方式，有效节省上网费用。
- 自动连接：若选择**自动连接**模式，则在开机后系统自动进行连接。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(30秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。

- 手动连接：选择该项，开机后需要用户手动才能进行拨号连接，若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按使用时间进行交费，可以选择该项连接方式。

完成更改后，点击保存按钮。

4.5.3 MAC地址克隆

选择菜单**网络参数→MAC地址克隆**，您可以在图 4-11界面中设置路由器对广域网的MAC地址。

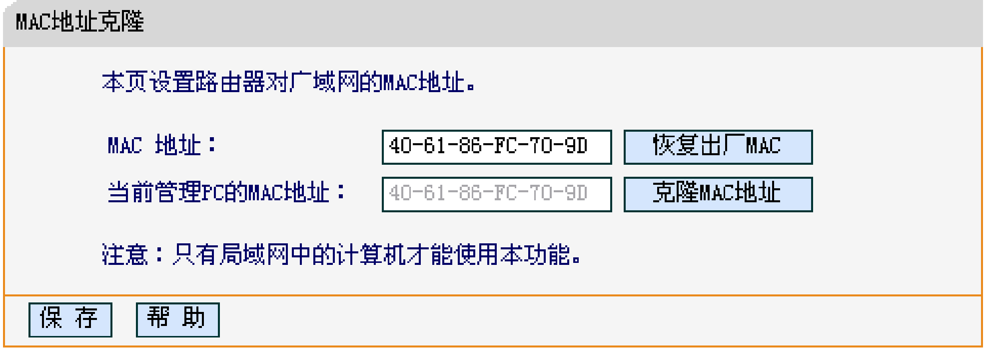


图 4-11 MAC 地址克隆

- MAC地址：此项为路由器对广域网的MAC地址，默认的MAC地址为路由器上WAN的物理接口MAC地址。某些ISP可能会要求对MAC地址进行绑定，此时ISP会提供一个有效的MAC地址给用户，您只要根据它所提供的值，输入到**MAC地址栏**。不建议更改MAC地址，除非ISP有特别要求。
- 当前管理PC的MAC地址：该处显示当前正在管理路由器的计算机的MAC地址。
- 恢复出厂MAC：单击此按钮，即可恢复MAC地址为出厂时的默认值。
- 克隆MAC地址：单击此按钮，可将当前管理PC的MAC地址克隆到**MAC地址栏**内。若您的ISP提供服务时要求进行MAC地址克隆，则可进行该项操作，否则无需克隆MAC地址。

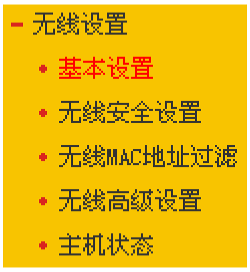
完成更改后，点击**保存**按钮，路由器会自动重启。

☞ 注意:

只有局域网中的计算机才能使用“MAC地址克隆”功能。

4.6 无线设置

选择菜单**无线设置**，您可以看到:



单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.6.1 基本设置

选择菜单**无线设置→基本设置**，您可以在图 4-12界面中设置无线网络的基本参数和安全认证选项。

无线功能是该路由器的一项重要功能，利用该功能，可以组建内部无线网络。组建网络时，内网主机需要一张无线网卡来连接无线网络。各项的详细设置情况见下面所述。

图 4-12 无线网络基本设置

- SSID：该项标识无线网络的网络名称。
- 信道：该项用于选择无线网络工作的频率段，可以选择的范围从1到13。
- 模式：该项用于设置您路由器的无线工作模式，推荐使用11bgn mixed模式。
- 频道带宽：设置无线数据传输时所占用的信道宽度，可选项为：20M、40M和自动。
- 最大发送速率：该项用于选择无线网络的最大发送速率。
- 开启无线功能：若要采用路由器的无线功能，必须选择该项，这样，无线网络内的主机才可以接入并访问有线网络。
- 开启SSID广播：该项功能用于将路由器的SSID号向无线网络内的主机广播，这样，主机将可以扫描到SSID号，并可以加入该SSID标识的无线网络。

完成更改后，点击**保存**按钮并重启路由器使现在的设置生效。

☞ 注意:

以上提到的频道带宽设置仅针对支持IEEE 802.11n协议的网络设备，例如，当本路由器与11N系列网卡客户端进行通信时；对于不支持IEEE 802.11n协议的设备，此设置不生效。

4.6.2 无线安全设置

选择菜单**无线设置→无线安全设置**，您可以在图 4-13界面中设置无线网络安全选项。

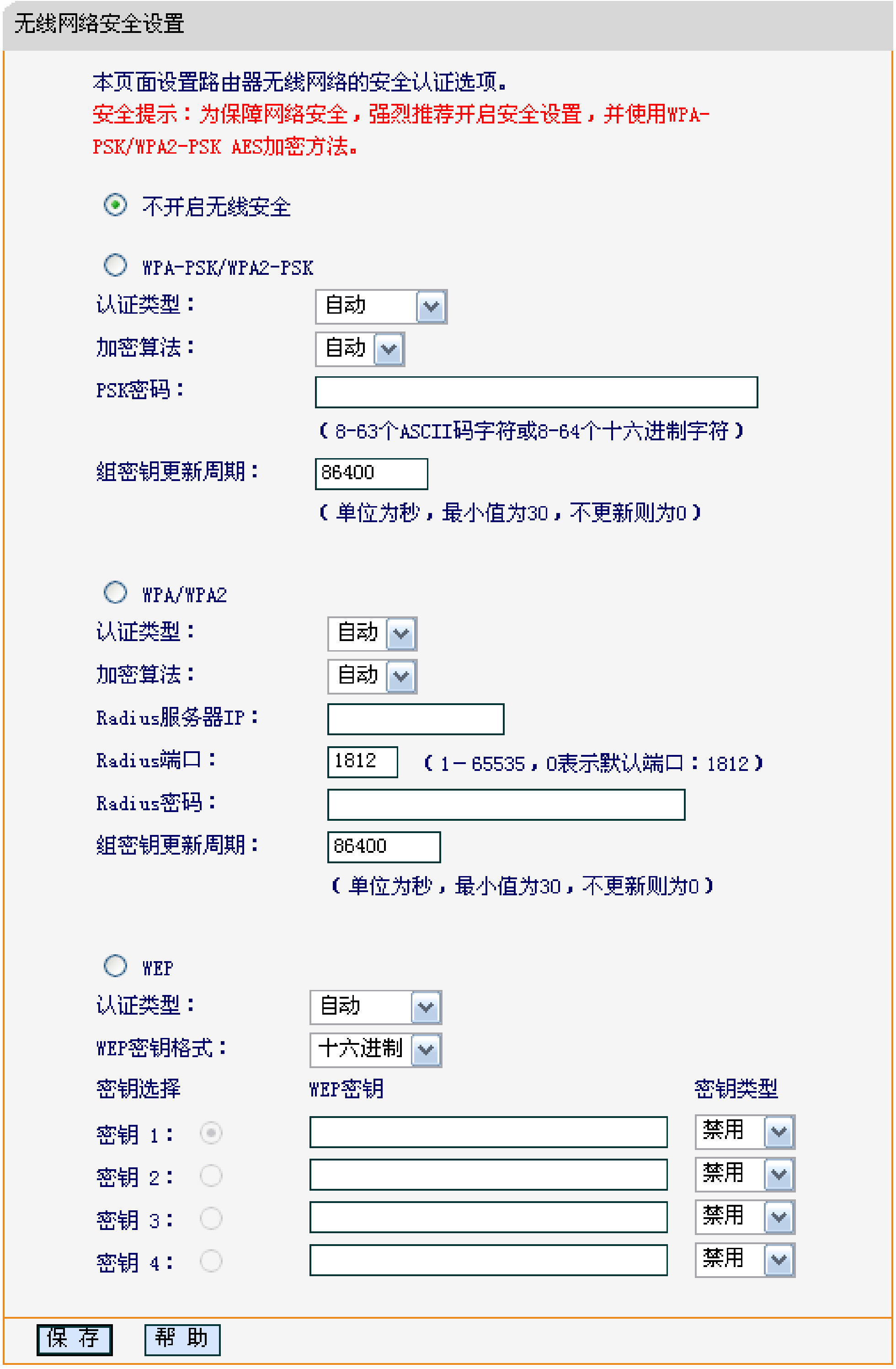


图 4-13 无线网络安全设置

在无线网络安全设置页面，您可以选择开启或者关闭无线安全功能。

- 如果您无需开启无线安全功能，请勾选关闭无线安全选项以关闭无线安全功能。
- 如果您要开启无线安全功能，则请选择页面中三种安全类型中的一种进行无线安全设置。

本页面提供了三种无线安全类型供您进行选择：WEP、WPA/WPA2 以及 WPA-PSK/WPA2-PSK。不同的安全类型下，安全设置项不同，下面将详细介绍。

1. WEP

选择WEP安全类型，路由器将使用IEEE 802.11基本的WEP安全模式。这里需要注意的是此加密方式经常在老的无线网卡上使用，而新的IEEE 802.11N不支持此加密方式。所以，如果您选择了此加密方式，路由器可能工作在较低的传输速率上。其具体设置项见下图所示。

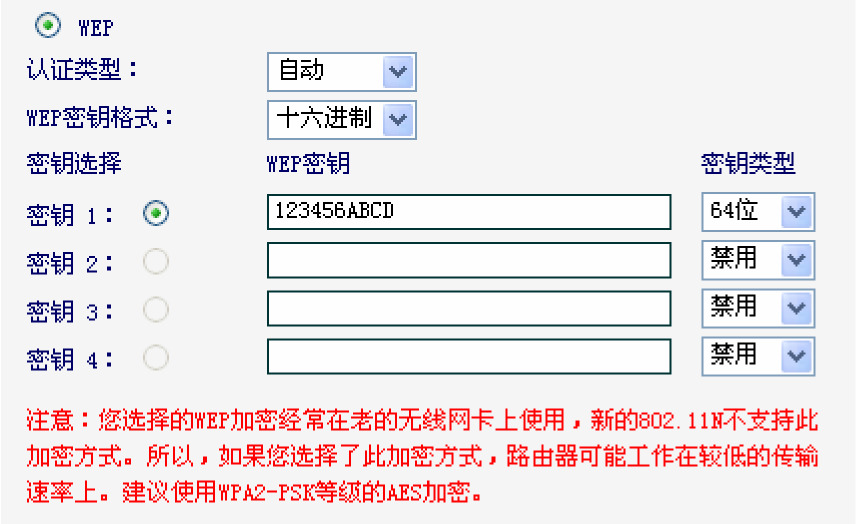


图 4-14 WEP 安全模式

- 认证类型：该项用来选择系统采用的安全方式，即自动、开放系统、共享密钥。
  - 自动：若选择该项，路由器会根据主机请求自动选择开放系统或共享密钥方式。
  - 开放系统：若选择该项，路由器将采用开放系统方式。此时，无线网络内的主机可以在不提供认证密码的前提下，通过认证并关联上无线网络，但是若要进行数据传输，必须提供正确的密码。
  - 共享密钥：若选择该项，路由器将采用共享密钥方式。此时，无线网络内的主机必须提供正确的密码才能通过认证，否则无法关联上无线网络，也无法进行数据传输。
- WEP密钥格式：该项用来选择即将设置的密钥的形式，即16进制、ASCII码。若采用16进制，则密钥字符可以为0～9，A、B、C、D、E、F；若采用ASCII码，则密钥字符可以是键盘上的所有字符。
- 密钥内容、密钥类型：这两项用来选择密钥的类型和具体设置的密钥值，密钥的长度受密钥类型的影响。

密钥长度说明：选择64位密钥需输入16进制字符10个，或者ASCII码字符5个。选择128位密钥需输入16进制字符26个，或者ASCII码字符13个。选择152位密钥需输入16进制字符32个，或者ASCII码字符16个。

2. WPA/WPA2

选择WPA/WPA2安全类型，路由器将采用Radius服务器进行身份认证并得到密钥的WPA或WPA2安全模式，其具体设置项见下图示。

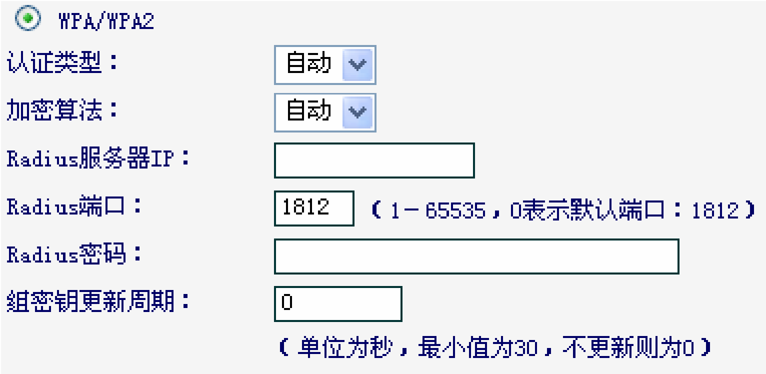


图 4-15 WPA/WPA2 安全模式

- 认证类型：该项用来选择系统采用的安全方式，即自动、WPA、WPA2。
  - 自动：若选择该项，路由器会根据主机请求自动选择WPA或WPA2安全模式。
  - WPA：若选择该项，路由器将采用WPA的安全模式。
  - WPA2：若选择该项，路由器将采用WPA2的安全模式。
- 加密算法：该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，路由器将根据实际需要自动选择TKIP或AES加密方式。这里需要注意的是，当您选择WPA/WPA2 TKIP加密在老的无线网卡上使用时，新的IEEE 802.11N不支持此加密方式，所以如果你选择了此加密方式，路由器可能工作在较低的传输速率上，建议使用WPA2-PSK等级的AES加密。如图4-16。

图 4-16 选择 WPA/WPA2 TKIP 加密

- Radius服务器IP：Radius服务器用来对无线网络内的主机进行身份认证，此项用来设置该服务器的IP地址。
- Radius端口：Radius服务器用来对无线网络内的主机进行身份认证，此项用来设置该Radius认证服务采用的端口号。
- Radius密码：该项用来设置访问Radius服务的密码。
- 组密钥更新周期：该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

3. WPA-PSK/WPA2-PSK

选择WPA-PSK/WPA2-PSK安全类型，路由器将采用基于共享密钥的WPA模式，其具体设置项见图 4-17示。

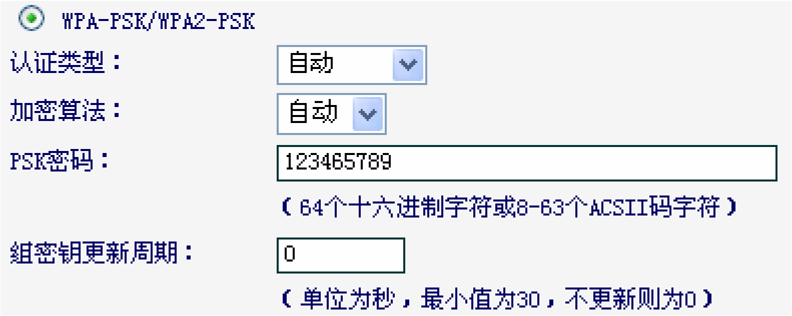


图 4-17 WPA-PSK/WPA2-PSK 安全模式

- 认证类型：该项用来选择系统采用的安全方式，即自动、WPA-PSK、WPA2-PSK。
  - 自动: 若选择该项, 路由器会根据主机请求自动选择WPA-PSK或WPA2-PSK安全模式。
  - WPA-PSK：若选择该项，路由器将采用WPA-PSK的安全模式。
  - WPA2-PSK：若选择该项，路由器将采用WPA2-PSK的安全模式。
- 加密算法：该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，路由器将根据实际需要自动选择TKIP或AES加密方式。注意11N模式不支持TKIP算法。
- PSK密码：该项是WPA-PSK/WPA2-PSK的初始设置密钥，设置时，要求为64个十六进制字符或8-63个ASCII码字符。
- 组密钥更新周期：该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

☞ 注意:

当路由器的无线设置完成后，无线网络内的主机若想连接该路由器，其无线设置必须与此处设置一致，如：SSID号。若该路由器采用了安全设置，则无线网络内的主机必须根据此处的安全设置进行相应设置，如密码设置必须完全一样，否则该主机将不能成功连接该路由器。

4.6.3 无线MAC地址过滤

选择菜单**无线设置→无线MAC地址过滤**，您可以在图 4-18界面中查看或添加无线网络的MAC地址过滤条目。

无线 MAC 地址过滤功能通过 MAC 地址允许或拒绝无线网络中的计算机访问广域网，有效控制无线网络内用户的上网权限。您可以利用按钮**添加新条目**来增加新的过滤规则；或者通过“编辑”、“删除”链接来编辑或删除旧的过滤规则。

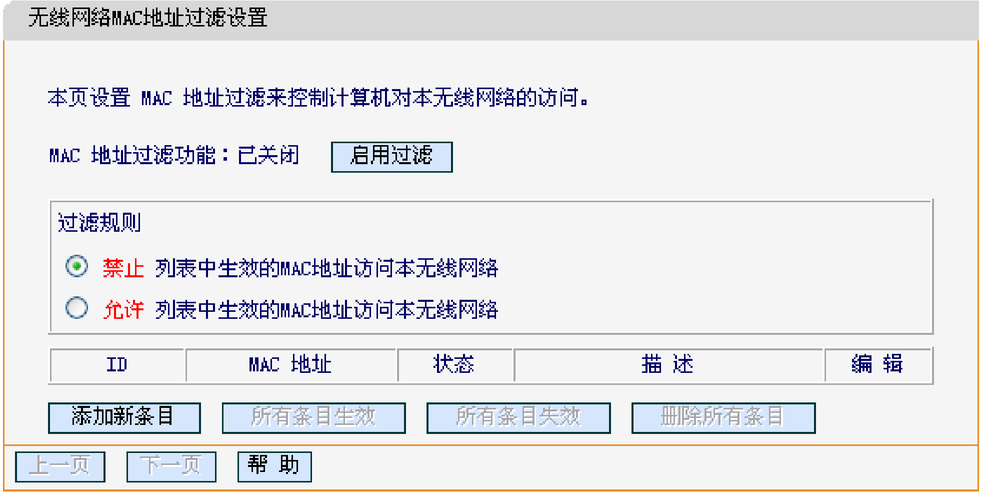


图 4-18 无线网络 MAC 地址过滤设置

- MAC地址过滤功能：请在该处选择是否开启路由器的无线网络MAC地址过滤功能。
- 过滤规则：请选择MAC地址过滤规则，该规则对下面MAC地址条目列表生效。
- MAC地址：该项指需要进行访问限制的无线网络内的主机MAC地址。
- 状态：该项显示MAC地址过滤条目的状态。“生效”表示该设置条目被启用，“失效”表示该设置条目未被启用。
- 描述：该项显示对主机的简单描述。
- 添加新条目：单击该项，您可以在随后的界面中添加新的MAC地址过滤条目。
- 使所有条目生效：单击该按钮，您可以使表中的所有条目生效。
- 使所有条目失效：单击该按钮，您可以使表中的所有条目失效。
- 删除所有条目：单击该按钮，您可以删除表中所有的条目。

例1： 如果您想禁止MAC地址为“00-0A-EB-00-07-BE”和“00-0A-EB-00-07-5F”的主机访问无线网络，其他主机可以访问无线网络，您可以按照以下步骤进行配置：

第一步：在图4-18中，选择过滤规则为“禁止列表中生效的MAC地址访问本无线网络”，并确认访问控制列表中没有任何生效的条目，如果有，将该条目状态改为“失效”或删除该条目，也可以点击**删除所有条目**按钮，将列表中的条目清空。

第二步：在图4-18中，点击**添加新条目**按钮，按照图4-19界面，设置MAC地址为“00-0A-EB-00-07-BE”，状态为“生效”。设置完成后，点击**保存**按钮。

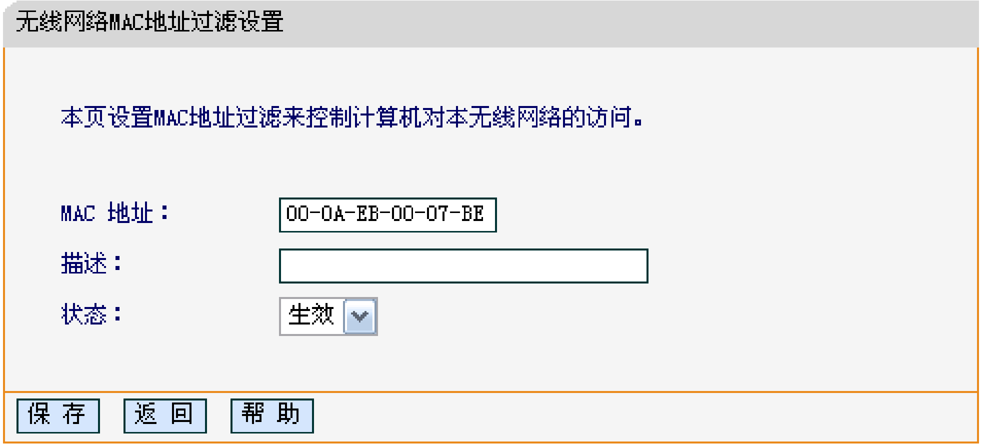


图 4-19 添加无线网络 MAC 地址过滤条目

第三步：参照第二步，继续添加过滤条目，设置MAC地址为“00-0A-EB-00-07-5F”，状态为“生效”。设置完成后，点击**保存**按钮。

第四步：在上图4-18中，点击**启用过滤**按钮，开启无线网络的访问控制功能。

例1中设置完成后生成的MAC地址过滤列表为：

ID	MAC地址	状态	描 述	编 辑
1	00-0A-EB-00-07-BE	生效		编辑 删除
2	00-0A-EB-00-07-5F	生效		编辑 删除

☞ 注意：

如果您开启了无线网络的MAC地址过滤功能，并且过滤规则选择了“允许列表中生效的MAC地址访问本无线网络”，而过滤列表中又没有任何生效的条目，那么任何主机都不可以访问本无线网络。

4.6.4 无线高级设置

选择菜单**无线设置→无线高级设置**，您可以看到如图 4-20的无线高级设置界面。

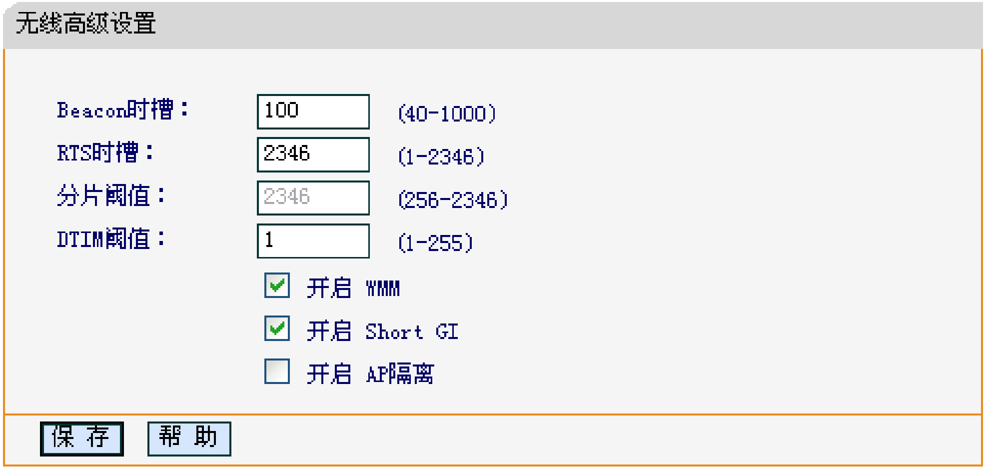


图 4-20 无线高级设置

- 传输功率：设置无线网络的传输功率，推荐保持默认值 “高”。
- Beacon时槽：路由器通过发送Beacon广播进行无线网络连接的同步。Beacon时槽表示路由器发送Beacon广播的频率。默认值为100毫秒。Beacon广播的取值范围是20－1000毫秒。
- RTS时槽：为数据包指定RTS（Request to Send，发送请求）阈值。当数据包长度超过RTS阈值时，路由器就会发送RTS到目的站点来进行协商。接收到RTS帧后，无线站点会回应一个CTS（Clear to Send，清除发送）帧来回应路由器，表示两者之间可以进行无线通信了。
- 分片阈值：为数据包指定分片阈值。当数据包的长度超过分片阈值时，会被自动分成多个数据包。过多的数据包将会造成网络性能降低，所以分片阈值不应设置过低。默认值为2346。
- DTIM阈值：该值在1至255毫秒之间，指定传输指示消息(DTIM)的间隔。 DTIM是一种倒数计时作业，用以告知下一个要接收广播及多播的客户端窗口。当路由器已经为相关联的客户端缓存了广播或者多播信息时，它就会传送夹带有下一个DTIM时槽的DTIM；当客户端听到Beacon讯号时，就会接收该广播和组播信息。默认值为1。

- 开启WMM：开启WMM后路由器具有无线服务质量(QOS)功能，可以对音频、视频数据优先处理，保证音频、视频数据的优先传输。推荐您勾选此项。
- 开启Short GI：选择此项可以使路由器接收和发送短帧间隔数据包，提高路由器的传输速率，推荐勾选。
- 开启AP隔离：选择此项可以隔离关联到AP的各个无线站点。

完成更改后，点击保存按钮。

4.6.5 主机状态

选择菜单**无线设置→主机状态**，您可以在图 4-21界面中查看当前连接到无线网络中的所有主机的基本信息。单击**刷新**按钮，您可以更新列表中的条目信息。

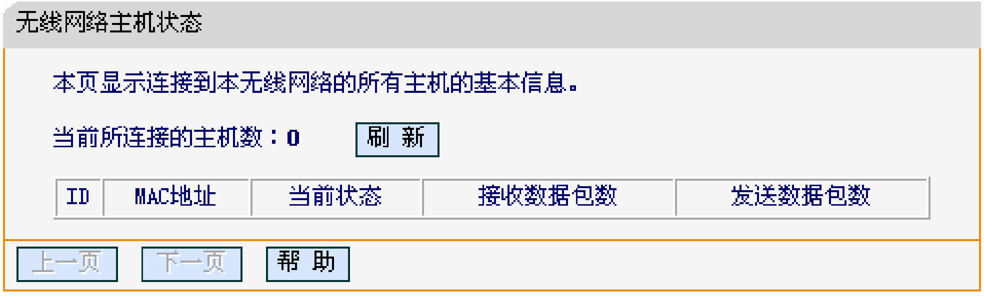


图 4-21 无线网络主机状态

- MAC地址：该处显示当前已经连接到无线网络的主机的MAC地址。
- 当前状态：此项显示当前主机的运行状态。
- 接收数据包数、发送数据包数：这两项显示当前主机接收和发送的数据包的总数。

4.7 DHCP服务器

选择菜单 **DHCP 服务器**，您可以看到：

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.7.1 DHCP服务

选择菜单**DHCP服务器→DHCP服务**，您将看到DHCP设置界面，如图 4-22。

DHCP指动态主机控制协议(Dynamic Host Control Protocol)。FW300R有一个内置的DHCP服务器，它能够自动分配IP地址给局域网中的计算机。对用户来说，为局域网中的所有计算机配置TCP/IP协议参数并不是一件容易的事，它包括IP地址、子网掩码、网关、以及DNS服务器的设置等。若使用DHCP服务则可以解决这些问题。您可以按照下面各子项说明正确设置这些参数。

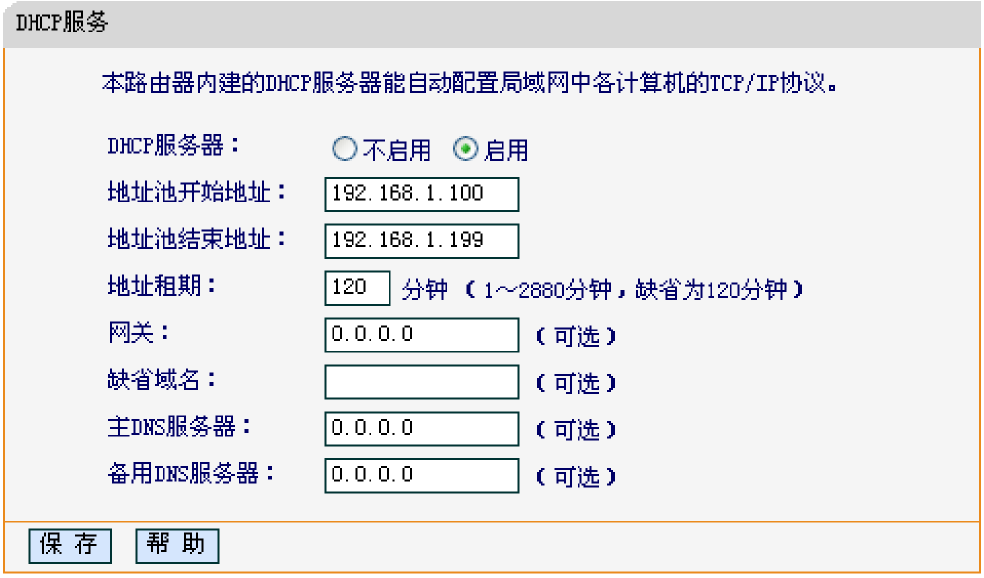


图 4-22 DHCP 服务

- 地址池开始地址、地址池结束地址：这两项为DHCP服务器自动分配IP地址时的起始地址和结束地址。设置这两项后，内网主机得到的IP地址将介于这两个地址之间。
- 地址租期：该项指DHCP服务器给客户端主机分配的动态IP地址的有效使用时间。在该段时间内，服务器不会将该IP地址分配给其它主机。
- 网关：此项应填入路由器LAN口的IP地址，缺省是192.168.1.1。
- 缺省域名：此项为可选项，应填入本地网域名(默认为空)。
- 主DNS服务器、备用DNS服务器：这两项为可选项，可以填入ISP提供给您的DNS服务器，不清楚可以向ISP询问。

完成更改后，点击**保存**按钮并重启路由器使现在的设置生效。

☞ 注意:

若要使用本路由器的DHCP服务器功能，局域网中计算机的TCP/IP协议项必须设置为"自动获得IP地址"。

4.7.2 客户端列表

选择菜单**DHCP服务器→客户端列表**，您可以查看所有通过DHCP服务器获得IP地址的主机的信息，单击**刷新**按钮可以更新表中信息，如图 4-23。

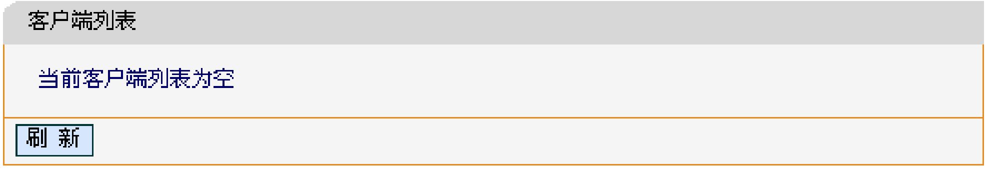


图 4-23 客户端列表

- 客户端名：该处显示获得了IP地址的客户端计算机的名称。
- MAC地址：该处显示获得了IP地址的客户端计算机的MAC地址。
- IP地址：该处显示DHCP服务器分配给客户端主机的IP地址。

- 有效时间：该项指客户端主机获得的IP地址离到期的时间，每个IP地址都有一定的租用时间，客户端软件会在租期到期前自动续约。

4.7.3 静态地址分配

选择菜单**DHCP服务器→静态地址分配**，您可以在图 4-24界面中设置静态IP地址。

静态地址分配功能可以为指定MAC地址的计算机预留静态IP地址。当该计算机请求DHCP服务器分配IP地址时，DHCP服务器将给它分配表中预留的IP地址。并且一旦采用，该主机的IP地址将不再改变。

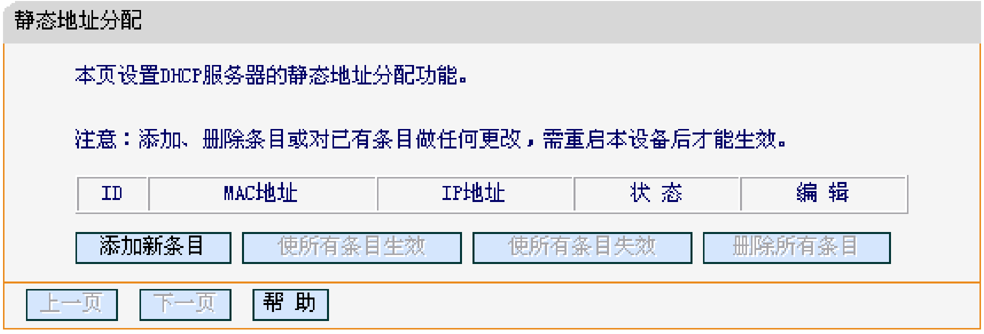


图 4-24 静态地址分配

- MAC地址：该项指定将要预留静态IP地址的计算机的MAC地址。
- IP地址：该项指定给内网主机预留的IP地址。
- 状态：显示该条目状态"生效"或"失效"，只有状态为生效时，本条过滤规则才生效。
- 添加新条目：单击该按钮，你可以在随后的界面中添加新的静态地址条目，如图4-25。
- 使所有条目生效：单击该按钮，您可以使表中的所有条目生效。
- 使所有条目失效：单击该按钮，您可以使表中的所有条目失效。
- 删除所有条目：单击该按钮，您可以删除表中所有的条目。

例1：如果您希望给局域网中MAC地址为00-13-8F-A9-6C-CB的计算机预留IP地址：192.168.1.101。这时您可以按照如下步骤设置：

第一步：在图4-24界面中单击**添加新条目**。

第二步：在图4-25界面中设置MAC地址为"00-13-8F-A9-6C-CB"，IP地址"192.168.1.101"，状态为"生效"。

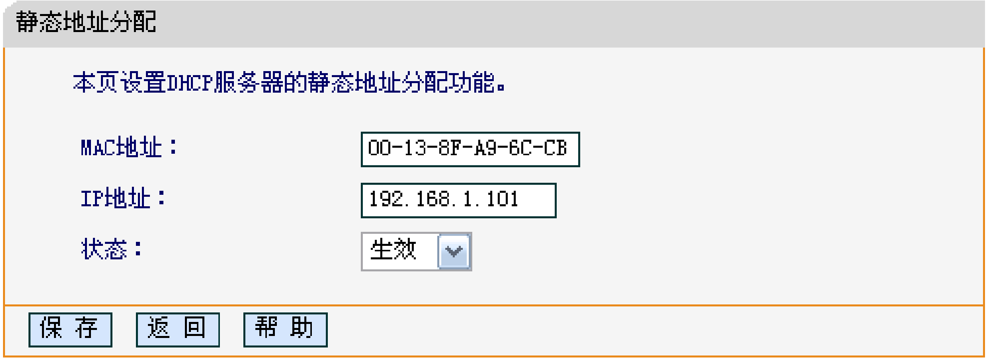
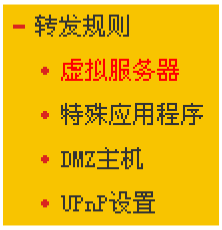


图 4-25 添加静态地址条目

第三步：点击**保存**按钮并重启路由器使现在的设置生效。

4.8 转发规则

选择菜单**转发规则**，您可以看到：



单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.8.1 虚拟服务器

选择菜单**转发规则→虚拟服务器**，您可以在图 4-26界面中设置虚拟服务器条目。

FW300R可配置为虚拟服务器，它能使通过公共IP地址访问Web或FTP等服务的远程用户自动转向到局域网中的本地服务器。

FW300R内置的防火墙特性能过滤掉未被识别的包，保护您的局域网络。在路由器默认设置下，局域网中所有的计算机都不能被外界看到。如果希望在保护局域网内部不被侵袭的前提下，某些LAN中的计算机在广域网上可见，请使用虚拟服务器。

虚拟服务器可以定义一个服务端口，外网所有对此端口的服务请求都将改发给路由器指定的局域网中的服务器(通过IP地址指定)，这样外网的用户便能成功访问局域网中的服务器，而不影响局域网内部的网络安全。

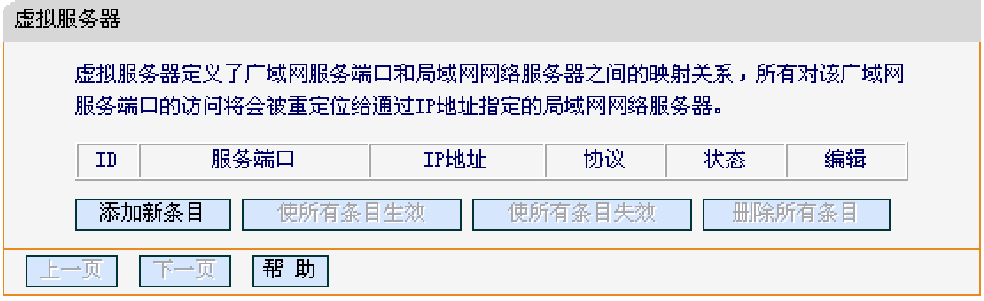


图 4-26 虚拟服务器

- 服务端口：此项为路由器提供给广域网的服务端口，广域网用户通过向该端口发送请求来获取服务。可输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，中间用“-”隔开。
- IP地址：局域网中被指定提供虚拟服务的服务器地址。
- 协议：虚拟服务所用的协议，可供选择的有：TCP、UDP和ALL。若对采用的协议不清楚，可以选择ALL。
- 状态：该项显示该条目状态“生效”或“失效”，只有状态为生效时，本条目的设置才生效。

例1：如果希望广域网用户通过端口21访问您的FTP服务器，FTP服务器在局域网中的IP地址为192.168.1.100，协议选择为TCP，则您可以按照如下步骤设置：

第一步：在图4-26界面中点击**添加新条目**按钮。

第二步：在图4-27界面中点击“常用服务端口号”下拉菜单，查找FTP服务，选中“FTP”服务。

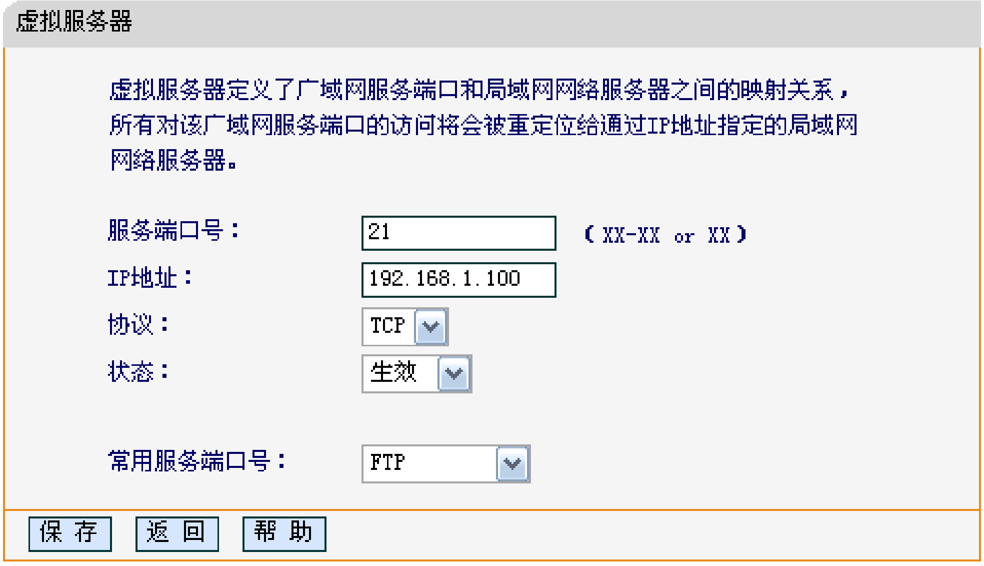


图 4-27 添加虚拟服务条目

- 常用服务端口号：在“常用服务端口号”中，列出了常用协议的端口，您可以直接从中选择一个，系统则会将该服务的端口号、协议类型，自动添加到对应序列的“服务端口号”和“协议”项中，您只需要再为其指定服务器IP地址并启用即可。对于常用服务端口中没有列出的端口，如果需要，也可以在服务端口处手动添加。

第三步：输入IP地址为“192.168.1.100”，设置条目状态为“生效”。

第四步：单击**保存**按钮。

设置好以后，您只要在局域网的服务器上进行相应的设置，广域网的计算机就可以访问到您局域网的服务器上了。

例2：如果希望广域网用户通过端口80访问您的Web服务器，Web服务器在局域网中的IP地址为192.168.1.101，协议选择为ALL，则您可以按照如下步骤设置：

第一步：在图4-26界面中点击**添加新条目**按钮。

第二步：在图4-27界面中设置服务端口为“80”，输入IP地址为“192.168.1.101”，选择协议为“ALL”。

第三步：点击**保存**按钮。

例1和例2设置完成后生成的虚拟服务列表为：

ID	服务端口	IP地址	协议	状态	编辑
1	21	192.168.1.100	TCP	生效	编辑 删除
2	80	192.168.1.101	ALL	生效	编辑 删除

☞ 注意：

如果设置了服务端口为80的虚拟服务器，则需要将安全设置→远端WEB管理的“WEB管理端口”设置为80以外的值，如88，否则会发生冲突，从而导致虚拟服务器不起作用。

例1中的服务在“常用服务端口”中已经提供，对于“常用服务端口”中没有提供的服务，可参照例2来添加。

4.8.2 特殊应用程序

选择菜单**转发规则→特殊应用程序**，您可以在图 4-28界面中设置特殊应用程序条目。

某些应用需要多条连接，如Internet网络游戏、视频会议、网络电话等。由于防火墙的存在，这些程序无法在简单的NAT路由器下工作。然而，特殊应用程序使得某些这样的应用程序能够在NAT路由器下工作。当一个应用程序向触发端口上发起连接时，对应的所有开放端口将会打开，以备后续连接并提供服务。

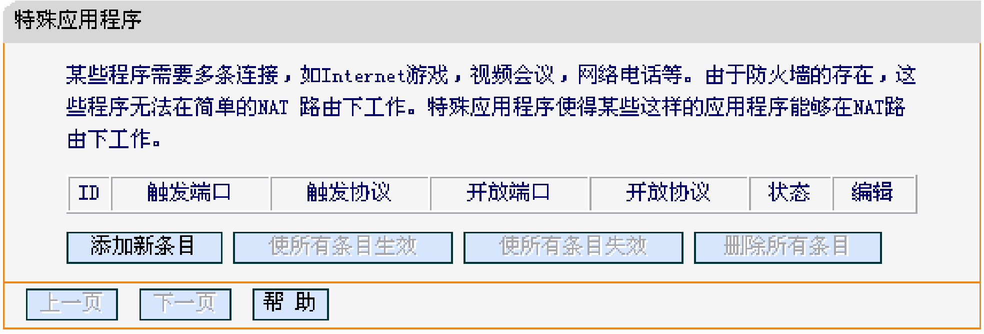


图 4-28 特殊应用程序

- 触发端口：该端口是应用程序首先发起连接的端口，只有在该端口上发起连接，开放端口中的所有端口才可以开放，否则开放端口是不会开放的。
- 触发协议：代表触发端口上使用的协议，可以选择ALL、UDP或TCP。若不清楚采用哪种协议，可以选用ALL。
- 开放端口：当向触发端口上成功发起连接后，对应的开放端口会打开，应用程序便可以向该开放端口发起后续的连接。此处可以输入一个或者多个端口或端口段，端口段输入格式为“开始端口-结束端口”，中间用“-”隔开，不同的端口段用“,”隔开。
- 开放协议：代表开放端口上使用的协议，可以选择ALL、UDP和TCP。若不清楚采用哪种协议，可以选用ALL。
- 状态：该项显示该条目状态“生效”或“失效”，只有状态为生效时，本条目的设置才生效。

在图 4-28界面中点击**添加新条目**按钮，您可以在图 4-29界面中添加新的特殊应用程序条目。

图 4-29 添加特殊应用程序条目

- 常用应用程序：在“常用应用程序”中，列出了常用的应用程序，您可以直接从中选择一个，系统则会自动将该常用应用程序的触发端口号和开放端口号添加到对应的“触发端口”和“开放端口”项中，并且会启用该条目。对于常用应用程序中没有列出的程序，您可以手动添加。

完成设置后，点击**保存**按钮。

4.8.3 DMZ主机

选择菜单**转发规则→DMZ主机**，您可以在图 4-30界面中设置DMZ(非军事区)主机。

局域网中设置DMZ主机后，该主机将完全暴露给广域网，可以实现双向无限制通信。具体设置时，只需输入局域网中指定为DMZ主机的IP地址，然后选中启用并点击保存即可。向DMZ添加客户机可能会给客户机带来不安全因素，因此请不要轻易使用这一选项。

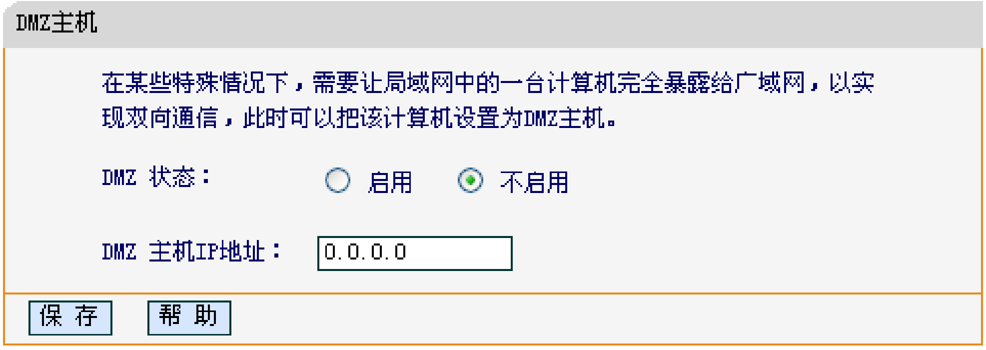


图 4-30 DMZ 主机

4.8.4 UPnP设置

选择菜单**转发规则→UPnP设置**，您可以在图 4-31界面中查看UPnP信息。

依靠UPnP(Universal Plug and Play)协议，局域网中的主机可以请求路由器进行特定的端口转换，使得外部主机能够在需要时访问内部主机上的资源，例如，Windows XP和Windows ME系统上安装的MSN Messenger，在使用音频和视频通话时就可以利用UPnP协议，这样原本受限于NAT的功能便可以恢复正常使用。

图 4-31 UPnP 设置

- 应用描述：应用程序通过UPnP向路由器请求端口转换时给出的描述。
- 外部端口：端口转换使用的路由器端口号。
- 协议类型：表明是对TCP还是UDP进行端口转换。

- 内部端口：需要进行端口转换的主机端口号。
- IP地址：需要进行端口转换的主机IP地址。
- 状态：该项显示条目是否已经启用。
- 刷新：单击该按钮，可以刷新当前的UPnP列表信息。

UPnP 的使用方法如下：

1. 点击**开启**按钮开启 UPnP 功能。
2. 当 MSN Messenger 等程序在运行中使用本功能时，按**刷新**按钮可以看到端口转换信息。端口转换信息由应用程序发出请求时提供。
3. 不使用时请点击**关闭**按钮关闭 UPnP 功能。

☞ 注意：

因为现阶段版本的UPnP协议的安全性还未得充分保证，在不需要时请关闭UPnP功能。

只有支持UPnP协议的应用程序才能使用本功能，MSN Messenger还可能需要操作系统的支持(如Windows ME/Windows XP/Windows Vista)。

UPnP功能需要操作系统的支持(如Windows ME/Windows XP/Windows Vista)。

4.9 安全设置

选择菜单**安全设置**，您可以看到：

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.9.1 防火墙设置

选择菜单**安全设置→防火墙设置**，您可以在下图 4-32界面中设置路由器的安全项。

该界面控制路由器防火墙总功能的开启，以及各子项功能：IP地址过滤、域名过滤和MAC地址过滤功能的开启和过滤规则。只有防火墙的总开关开启后，后续的安全设置才能够生效，反之，则不能生效(建议在过滤规则设置完成后再开启防火墙总开关)。

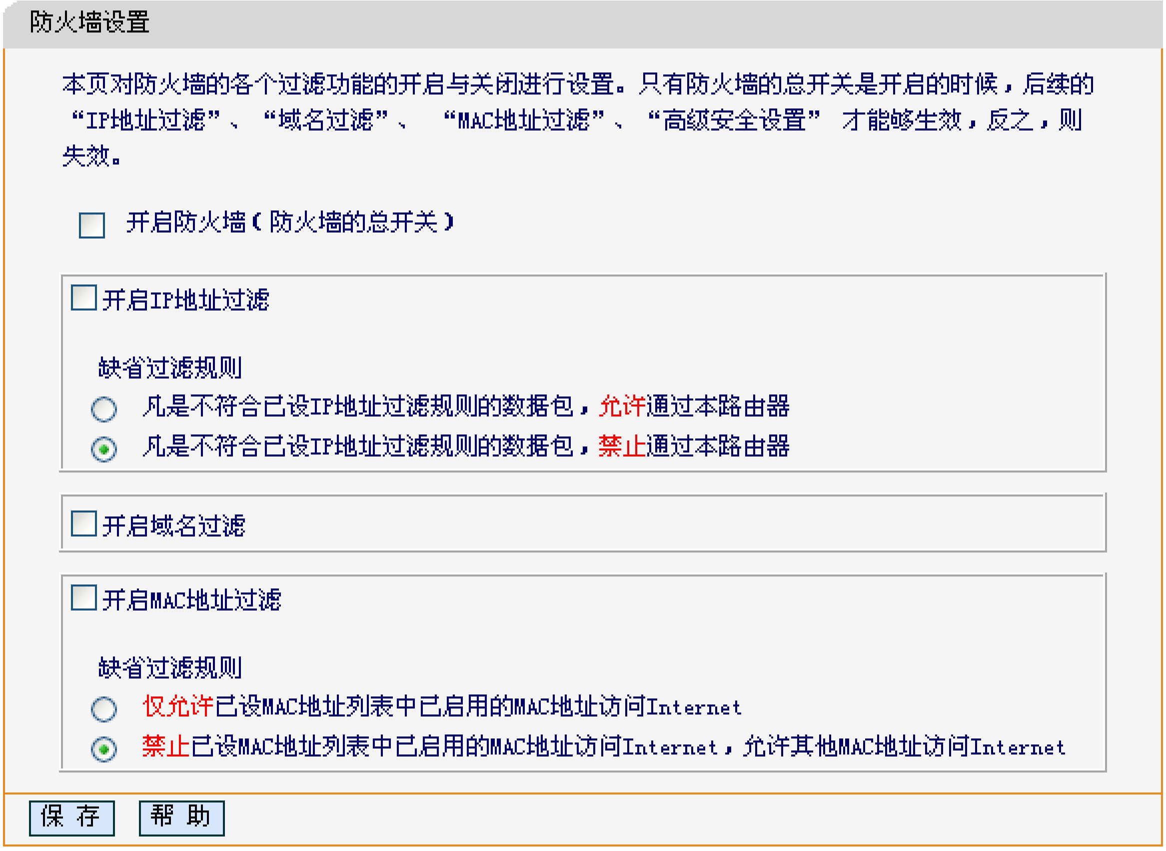


图 4-32 防火墙设置

- 开启防火墙：这是防火墙的总开关，只有该项开启后，IP地址过滤、域名过滤、MAC地址过滤功能才能启用，反之，则不能被启用。
- 开启IP地址过滤：关闭或开启IP地址过滤功能并选择缺省过滤规则。只有“开启防火墙”启用后，该项才能生效。
- 开启域名过滤：关闭或开启域名过滤功能。只有“开启防火墙”启用后，该项才能生效。
- 开启MAC地址过滤：关闭或开启MAC地址过滤功能并选择缺省过滤规则。只有“开启防火墙”启用后，该项才能生效。

完成设置后，点击**保存**按钮。

4.9.2 IP地址过滤

选择菜单**安全设置→IP地址过滤**，您可以在下图 4-33界面中查看并添加IP地址过滤条目。

使用IP地址过滤可以拒绝或允许局域网中计算机与互联网之间的通信。可以拒绝或允许特定IP地址的特定的端口号或所有端口号。

您可以利用按钮**添加新条目**来增加新的过滤规则，或者通过“修改”、“删除”链接来修改或删除已设过滤规则，甚至可以通过按钮**移动**来调整各条过滤规则的顺序，以达到不同的过滤优先级(ID序号越靠前则优先级越高)。

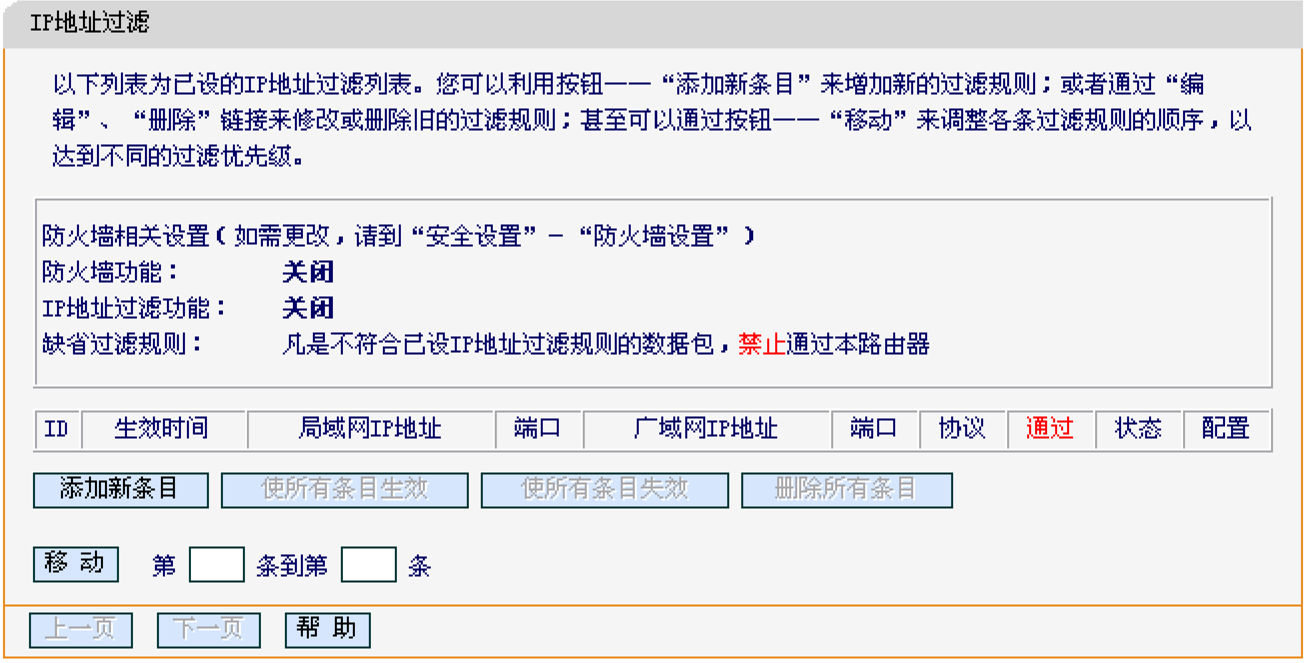


图 4-33 IP 地址过滤

- 生效时间：该项用来指定过滤条目的有效时间，在该段时间外，此过滤条目不起作用。
- 局域网IP地址：局域网中被控制的计算机的IP地址，为空表示对局域网中所有计算机进行控制。此处可以输入一个IP地址段，例如：192.168.1.123 – 192.168.1.185。
- (局域网)端口：局域网中被控制的计算机的服务端口，为空表示对该计算机的所有服务端口进行控制。此处可以输入一个端口段，例如：1030 – 2000。
- 广域网IP地址：广域网中被控制的计算机(如网站服务器)的IP地址，为空表示对整个广域网进行控制。此处可以输入一个IP地址段，例如：61.145.238.6-61.145.238.47。
- (广域网)端口：广域网中被控制的计算机(如网站服务器)的服务端口，为空表示对该网站所有服务端口进行控制。此处可以输入一个端口段，例如：25-110。
- 协议：此处显示被控制的数据包所使用的协议。
- 通过：该项显示符合本条目所设置的规则的数据包是否可以通过路由器，“是”表示允许该条目通过路由器，“否”表示不允许该条目通过路由器。
- 状态：显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则才生效。

例1：如果您希望禁止局域网中IP地址为192.168.1.7的计算机在8：30到18：00之间收发邮件，禁止IP地址为192.168.1.8的计算机在8：00到18：00之间访问IP为202.96.134.12的网站，对局域网中的其它计算机则不做任何限制，这时您可以按照如下步骤设置：

第一步：在图4-32界面中打开防火墙总开关。

第二步：在图4-32中开启“IP地址过滤”，设置“缺省过滤规则”为“凡是不符合已设IP地址过滤规则的数据包，允许通过本路由器”。

第三步：在图4-33界面中点击**添加新条目**，然后在下图4-34中按要求添加过滤条目。下图是禁止192.168.1.7的计算机在8：30到18：00之间发送邮件的设置，设置完成后点击**保存**按钮。

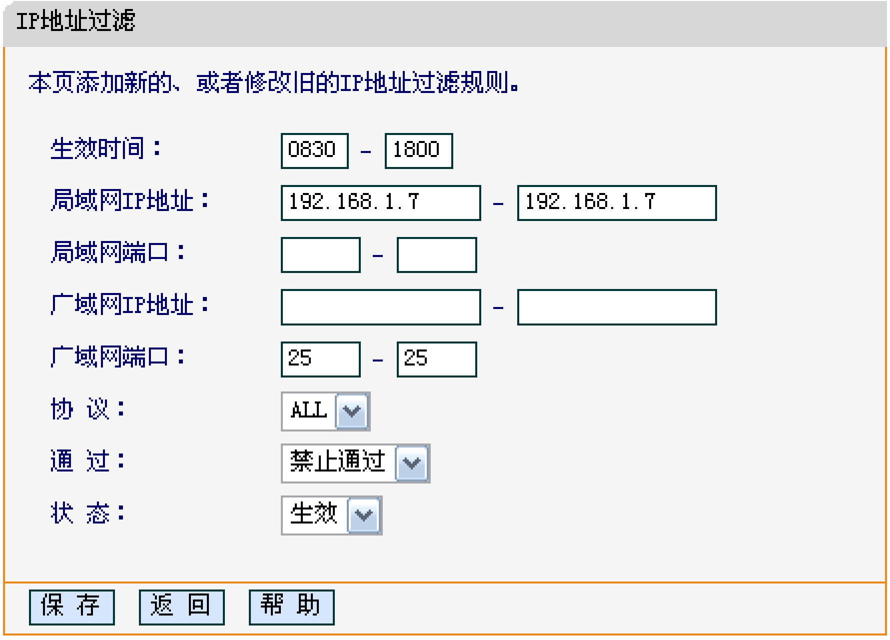


图 4-34 添加 IP 地址过滤条目

第四步：回到第三步，继续设置过滤条目：禁止局域网中IP地址为192.168.1.7的计算机在8：30到18：00之间接收邮件，禁止IP地址为192.168.1.8的计算机在8：00到18：00之间访问IP为202.96.134.12的网站。完成例1中设置一共需要设置3条IP过滤规则，依次对应下面列表中的三条过滤条目。

ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0830-1800	192.168.1.7-	-	-	25-	ALL	否	生效	编辑 删除
2	0830-1800	192.168.1.7-	-	-	110-	ALL	否	生效	编辑 删除
3	0830-1800	192.168.1.8-	-	202.96.134.12-	-	ALL	否	生效	编辑 删除

4.9.3 域名过滤

选择菜单**安全设置→域名过滤**，您可以在下图 4-35界面中查看并添加域名过滤条目。

域名过滤可以阻止LAN中所有计算机访问广域网(如互联网)上的特定域名，该特性会拒绝所有到特定域名如http和ftp的请求。您可以利用按钮**添加新条目**来增加新的过滤规则，或者通过"修改"、"删除"链接来修改或删除旧的过滤规则。

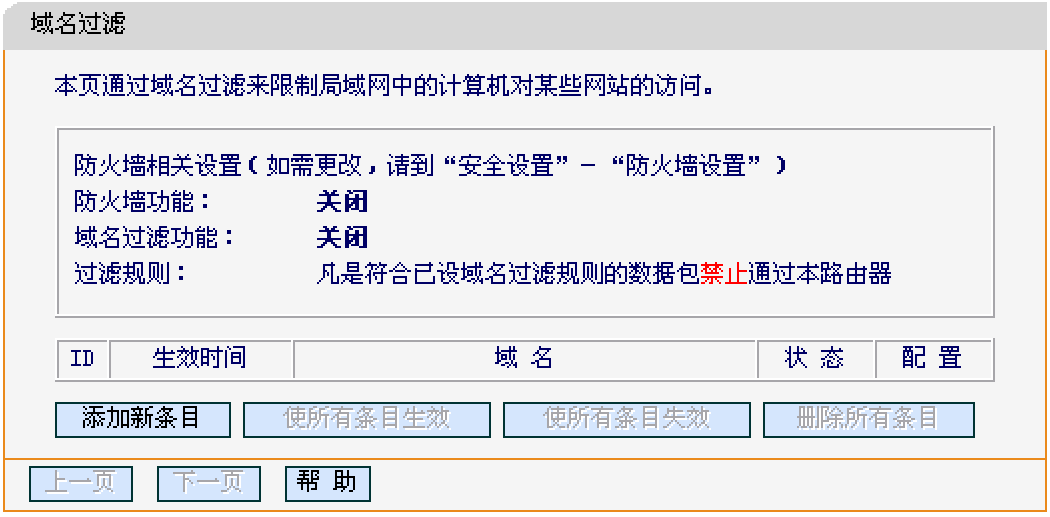


图 4-35 域名过滤

- 域名：拒绝被LAN计算机访问的域名。
- 状态：显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则才生效。

例1：如果您希望禁止局域网中的计算机在8：30到18：00之间访问“www.yahoo.com.cn”、“sina.com”的网站，禁止局域网中的计算机在8：00到12：00之间访问所有以“.net”结尾的网站，这时您可以按照如下步骤设置：

第一步：在图4-32界面中打开防火墙总开关并开启“域名过滤”。

第二步：在图4-35界面中点击**添加新条目**，然后在下图4-36界面中设置条目信息。下图是在8：30到18：00之间拒绝访问www.yahoo.com.cn网站的设置，设置完成后，点击保存按钮。

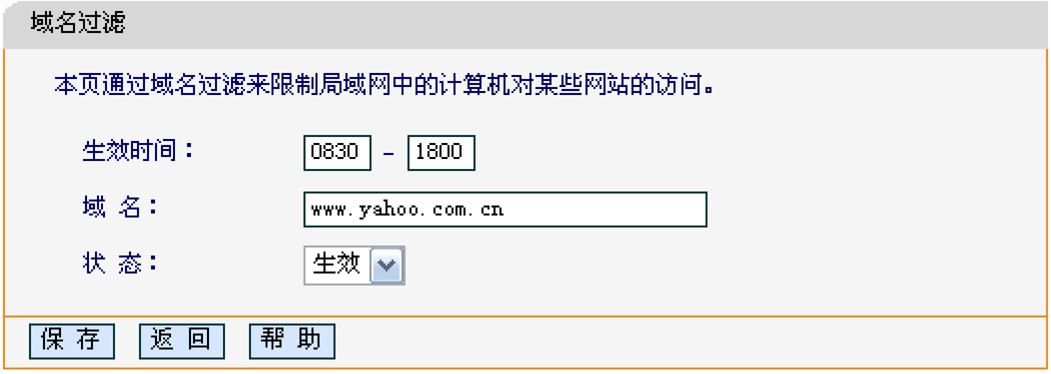


图 4-36 添加域名过滤条目

第三步：回到第二步，继续设置过滤条目：禁止局域网中的计算机在8：30到18：00之间访问“sina.com”，禁止局域网中的计算机在8：00到12：00之间访问所有以“.net”结尾的网站。完成例1中设置一共需要设置3条域名过滤规则，依次对应下面列表中的三条过滤条目。

ID	生效时间	域 名	状 态	配 置
1	0830-1800	www.yahoo.com.cn	生效	编辑 删除
2	0830-1800	sina.com	生效	编辑 删除
3	0830-1800	.net	生效	编辑 删除

4.9.4 MAC地址过滤

选择菜单**安全设置→MAC地址过滤**，您可以在下图 4-37界面中查看并添加MAC地址过滤条目。

MAC地址过滤功能通过MAC地址允许或拒绝局域网中计算机访问广域网，有效控制局域网内用户的上网权限。您可以利用按钮**添加新条目**来增加新的过滤规则；或者通过"修改"、"删除"链接来修改或删除旧的过滤规则。

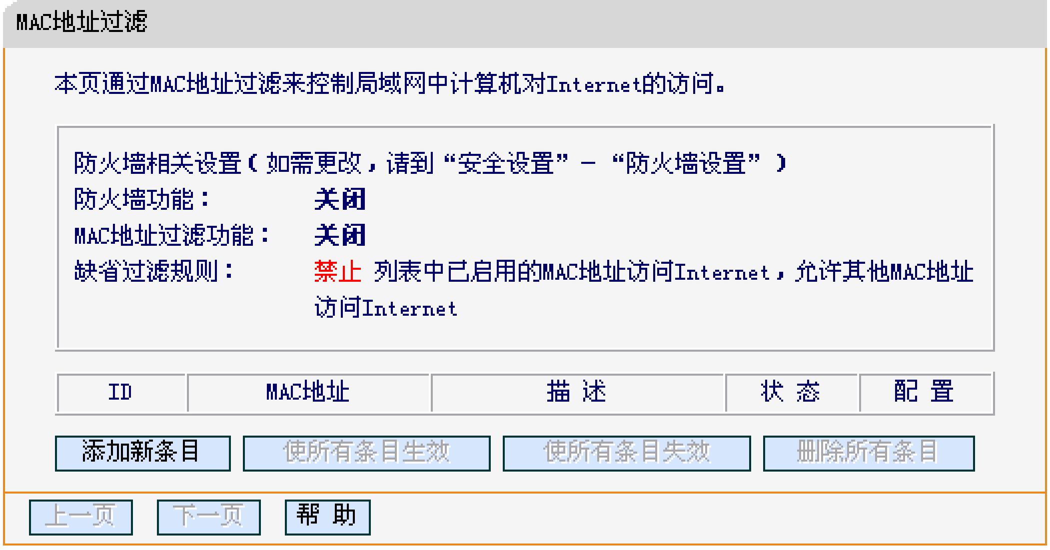


图 4-37 MAC 地址过滤

- MAC地址：该项是您希望管理的计算机的MAC地址。
- 描述：该项是对该计算机的适当描述。
- 状态：显示该条目状态"生效"或"失效"，只有状态为生效时，本条过滤规则才生效。

例1：如果您不希望局域网中MAC地址为00-E0-4C-00-07-BE和00-E0-4C-00-07-5E的计算机访问Internet，而希望局域网中的其它计算机能访问Internet，这时您可以按照如下步骤设置MAC地址过滤表：

第一步：在图 4-32界面中打开防火墙总开关。

第二步：在图 4-32防火墙设置界面中开启"MAC地址过滤"，设置"缺省过滤规则"为"禁止已设MAC地址列表中已启用的MAC地址访问Internet，允许其它MAC地址访问Internet"。

第三步：在图 4-37界面中点击**添加新条目**，然后在下图 4-38界面中设置条目信息。下图是禁止MAC地址为 00-E0-4C-00-07-BE的计算机访问Internet的设置，设置完成后，点击**保存**按钮。

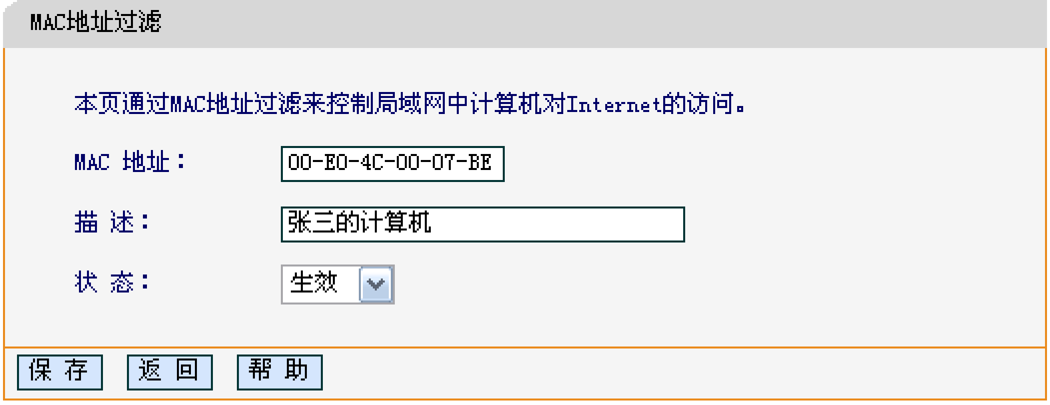


图 4-38 添加 MAC 地址过滤条目

第四步：回到第三步，继续设置过滤条目：禁止 MAC 地址为 00-E0-4C-00-07-5E 的计算机访问 Internet。完成例 1 中设置一共需要设置 2 条域名过滤规则，依次对应如下列表中的 2 条过滤条目。

ID	MAC地址	描 述	状 态	配 置
1	00-E0-4C-00-07-BE	张三的计算机	生效	编辑 删除
2	00-E0-4C-00-07-5E	李四的计算机	生效	编辑 删除

4.9.5 远端WEB管理

选择菜单**安全设置→远端WEB管理**。远端WEB管理功能可以允许用户通过Web浏览器从广域网配置路由器。本特性允许您从远程主机执行管理任务。您可以在下图 4-39界面中设置管理IP地址和端口。

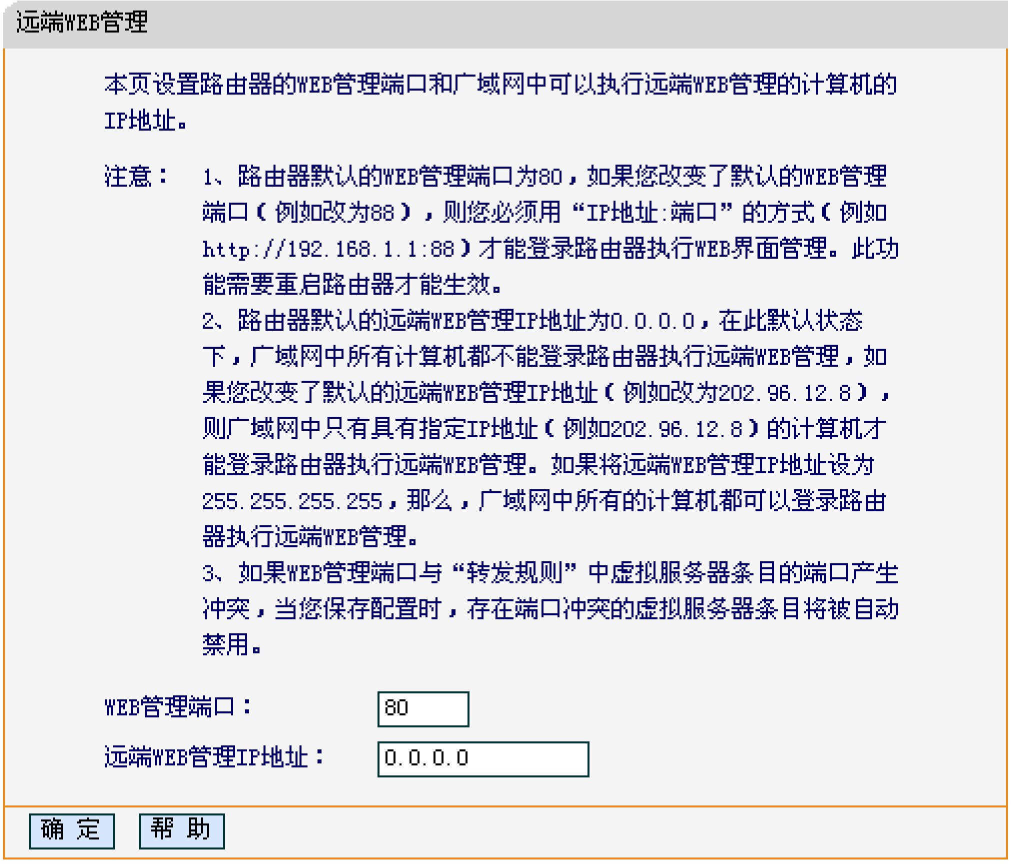


图 4-39 远端 WEB 管理

- WEB管理端口：用于访问宽带路由器的WEB管理端口号。
- 远端WEB管理IP地址：广域网中可以访问该路由器执行远端WEB管理的计算机IP地址。

完成更改后，点击**保存**按钮。

☞ 注意:

1. 路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口(例如改为88)，则您必须用“IP地址:端口”的方式(例如http://192.168.1.1:88)才能登录路由器执行WEB界面管理。此功能需要重启路由器后才生效。
2. 路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB管理IP地址(则广域网中只有具有该指定IP地址的计算机才能登录路由器执行远端WEB管理。如果改为255.255.255.255，则WAN中所有主机都可以登录路由器执行远端WEB管理。

例1: 如果您希望广域网中IP地址为202.96.134.13的计算机能够访问宽带路由器，执行远端WEB管理功能，WEB管理端口为80。则您可以进行如下设置:

第一步：设置 WEB 管理端口为“80”。

第二步：设置远端 WEB 管理 IP 地址为“255.255.255.255”或“202.96.134.13”。

这样，该计算机访问路由器管理界面时应该输入路由器WAN口IP地址即可。

4.9.6 高级安全设置

选择菜单**安全设置→高级安全设置**，您可以在下图 4-40界面中开启DoS(拒绝服务)攻击防范。完成更改后，点击**保存**按钮。

DoS攻击的目的是用极大量的虚拟信息流耗尽目标主机的资源，受害者被迫全力处理虚假信息流，从而影响对正常信息流的处理。如果DoS攻击始发自多个源地址，则称为分布式拒绝服务(DDoS) 攻击。通常DoS与DDoS攻击中的源地址都是欺骗性的。

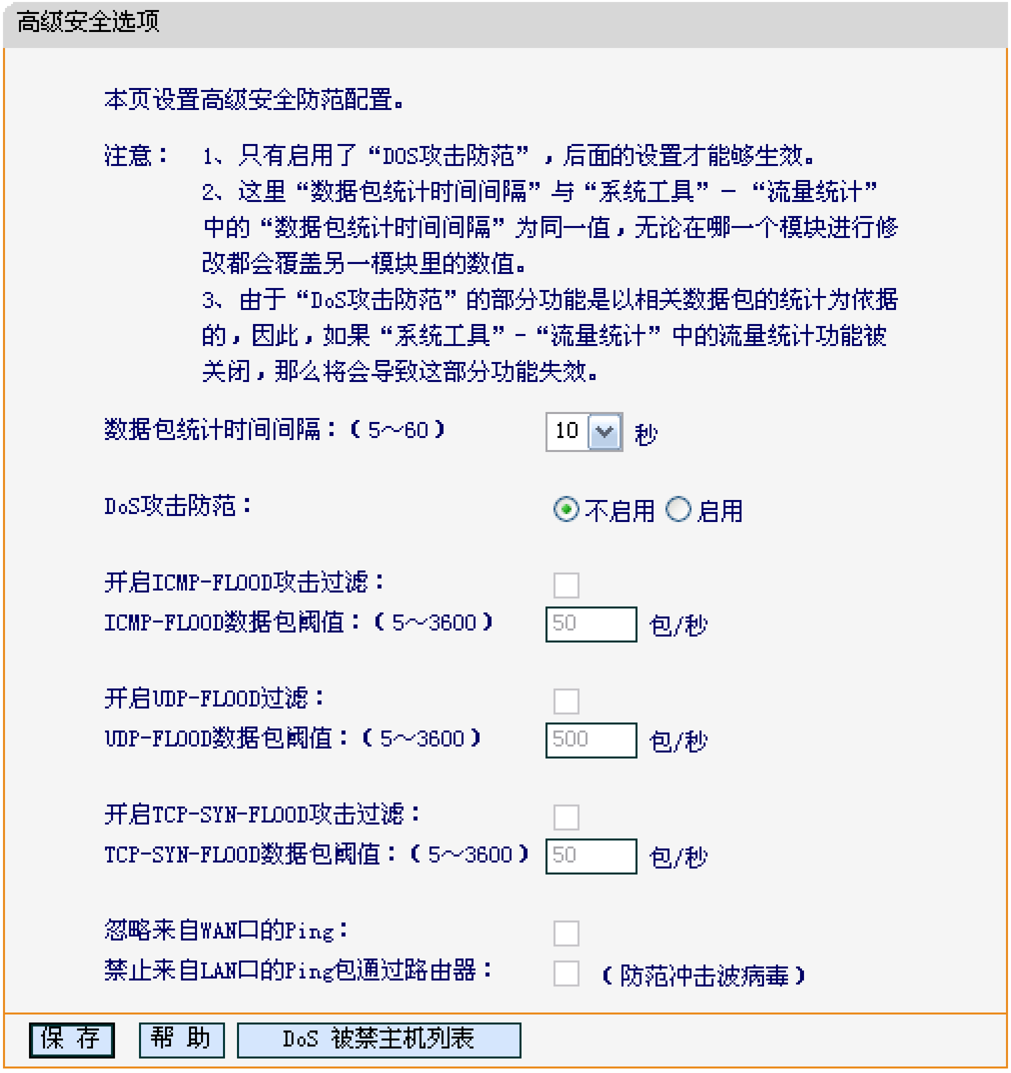


图 4-40 WAN 口 Ping

- 数据包统计时间间隔：该项设置对ICMP、UDP、TCP数据包进行统计的时间间隔，即在当前时间间隔内对各种数据包进行统计，如果统计得到的某种数据包(例如UDP FLOOD)达到了指定的阈值，那么系统将认为UDP-FLOOD 攻击已经发生，如果UDP-FLOOD过滤已经开启，那么路由器将会停止接收该类型的数据包,从而达到防范攻击的目的。
- DoS攻击防范：该项是开启下面各种攻击防范的总开关，只有选择此项后，以下的几种防范措施才能生效。
- 开启ICMP-FLOOD攻击过滤：若需要防范ICMP-FLOOD攻击，请选择此项。
- ICMP-FLOOD数据包阈值：当开启ICMP-FLOOD功能后，如果在指定时间间隔内ICMP包达到了指定的数目，防范措施则立即启动。
- 开启UDP-FLOOD攻击过滤：若需要防范UDP-FLOOD，请选择此项。
- UDP-FLOOD数据包阈值：当开启UDP-FLOOD功能后，如果在指定时间间隔内UDP包达到了指定的数目，防范措施则立即启动。
- 开启TCP-SYN-FLOOD攻击过滤：若需要防范TCP-SYN-FLOOD，请选择此项。
- TCP-SYN-FLOOD数据包阈值：当开启TCP-SYN-FLOOD功能后，如果在指定时间间隔内TCP的SYN包达到了指定的数目，防范措施则立即启动。

- 忽略来自WAN口的Ping：若开启该功能，广域网的计算机将不能Ping通路由器。
- 禁止来自LAN口的Ping包通过路由器：若开启该功能，局域网的计算机将不能Ping通广域网中的计算机。
- DoS被禁主机列表：点击该按钮，你可以查看被禁止的主机列表，如图4-41。单击**刷新**按钮可以更新列表信息。若希望被禁主机能够重新上网，可以点击**删除**按钮；若需要释放所有被禁主机，可以点击**清空**按钮。

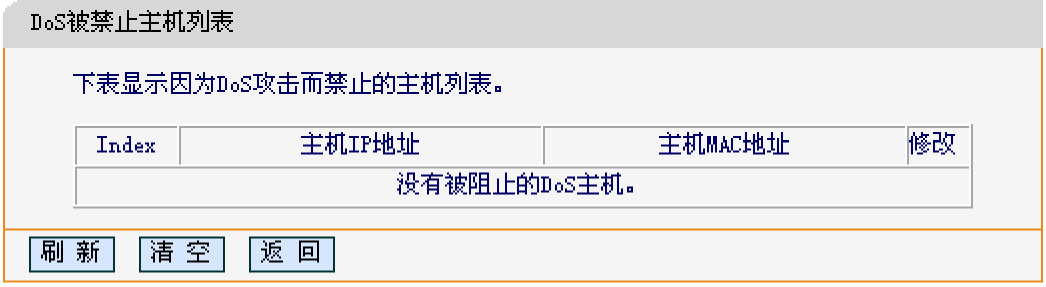


图4-41 DoS被禁主机列表

4.10 路由功能

选择菜单**路由功能**，您可以看到：

单击**静态路由表**，您即可进行静态路由功能设置，下面将详细讲解静态路由功能的设置。

4.10.1 静态路由表

选择菜单**路由功能→静态路由表**，您可以在图 4-42的界面中设置静态路由信息。

静态路由是一种特殊的路由，在网络中使用合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。通过设定目的IP地址、子网掩码和网关地址可以确定一个路由条目，其中目的IP地址和子网掩码用来确定一个目标网络/主机，之后路由器会通过网关将数据包发往指定的目标网络/主机。

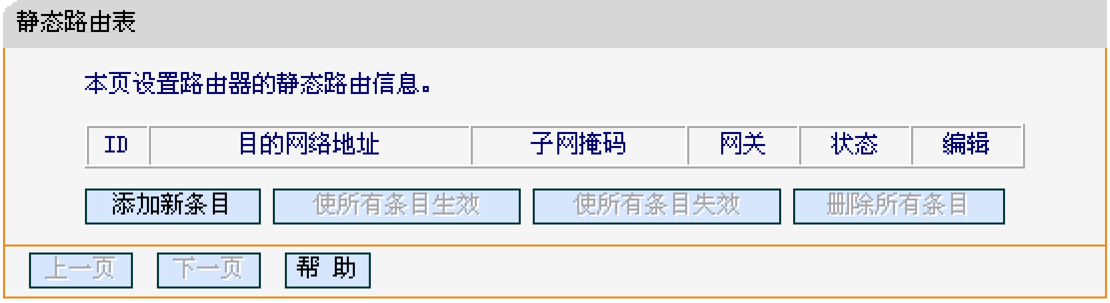


图 4-42 静态路由表

- 目的IP地址：用来标识希望访问的目标地址或目标网络。
- 子网掩码：该项与目的IP地址一起来标识目标网络，把目标地址和网络掩码逻辑与即可得到目标网络。

- 网关：数据包被发往的路由器或主机的IP地址。
- 状态：显示该条目是否生效，只有状态为生效时，此路由条目才起作用。
- 添加新条目：点击该项，你可以在图4-43中添加静态路由条目。

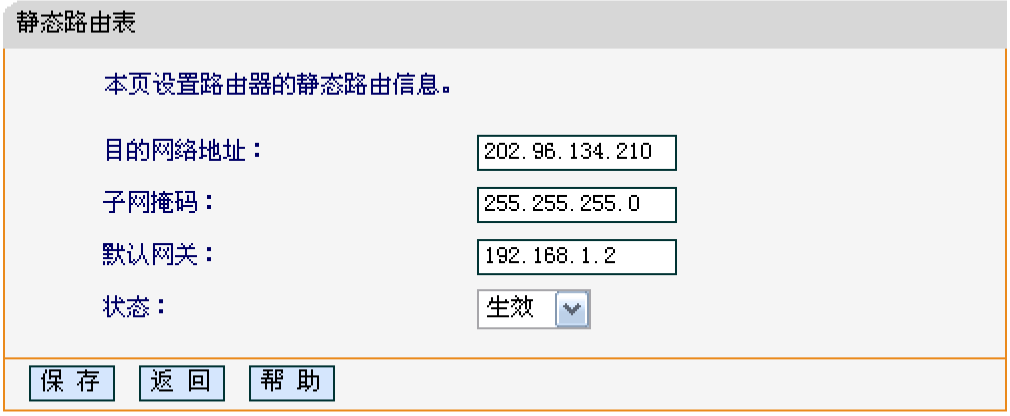


图 4-43 添加静态路由条目

完成设置后，点击保存按钮。

☞ 注意:

设置静态路由条目时，目的IP地址不能和路由器的WAN口或LAN口IP地址处于同一网段。

4.11 IP带宽控制

带宽控制功能可以实现对局域网计算机上网带宽的控制。在带宽资源不足的情况下，通过对各类数据包的带宽进行控制，可以实现带宽的合理分配，达到有效利用现有带宽的目的。通过 IP 带宽控制功能，可以设置局域网内主机的带宽上下限，保证每台主机都能通畅地共享网络，并在网络空闲时充分利用网络带宽。

选择菜单**IP带宽控制**，将进入下图 4-44所示界面。在此界面中，您可以开启或关闭IP带宽控制功能，并设置IP带宽控制规则。

图 4-44 IP 带宽控制设置功能设置

- 开启IP带宽控制：选择是否开启IP带宽控制功能，只有此处开启时，后续的“控制规则”设置才能够生效。
- 带宽线路类型：您申请的带宽线路类型，此处仅区分ADSL线路和其它线路。
- 申请的带宽大小：您申请的带宽大小，如果此处填写的值与实际不符，IP带宽控制功能可能会受影响。

以下为IP带宽控制规则列表中的各项说明：

- IP地址段：受该条规则限制的IP地址（或IP地址段），不同规则的IP地址不能有交集。
- 模式：对该条规则中的IP地址（或IP地址段）进行限制的方式。
- 带宽大小：如果该条规则的模式为“保障最小带宽”，受该条规则限制的IP地址（或IP地址段）的带宽总和至少可以达到此值；如果该条规则的模式为“限制最大带宽”，受该条规则限制的IP地址（或IP地址段）的带宽总和最多只能达到此值。
- 备注：对该条规则的文字说明，不超过10个字（包括标点符号）。
- 启用：是否启用该条规则。

完成设置后，点击保存按钮。

4.12 IP与MAC绑定

选择菜单 **IP 与 MAC 绑定菜单**，您可以看到：

单击某个子项，您即可进行相应功能的设置，下面将详细讲解两个子项的功能。

4.12.1 静态ARP绑定设置

选择**IP与MAC绑定→静态ARP绑定设置**，即可进入图 4-45的设置界面设置静态ARP绑定条目。
ARP 绑定主要是将主机的 IP 地址与相应的 MAC 地址进行绑定，是防止 ARP 欺骗的有效方法。在路由器中设置静态 ARP 绑定条目，可以维护内网用户的上网安全。当主机向路由器发送 ARP 请求时，路由器会根据主机的 IP 地址去查看 ARP 静态绑定列表，若列表中的 MAC 地址与主机的 MAC 地址相同，则路由器会允许该 ARP 请求，否则将不允许该请求。
要使用 ARP 绑定功能，您需要先设置以下项目：

图 4-45 静态 ARP 绑定设置

- ARP绑定：该项用来开启ARP绑定功能，只有选择"启用"时，列表中的设置才能生效。
- MAC地址：该项显示被绑定主机的MAC地址。
- IP地址：该项显示被绑定主机的IP地址。
- 绑定：该项显示条目状态，只有选中该项，该条绑定条目才能生效。

例1：如果您希望将某台主机的IP地址和MAC地址进行绑定，其IP地址为192.168.1.100，MAC地址为00-19-66-80-54-36，这时您可以按照如下步骤设置：

第一步：在图4-45界面中点击**增加单个条目**。

第二步：按照图4-46界面设置MAC地址和IP地址。

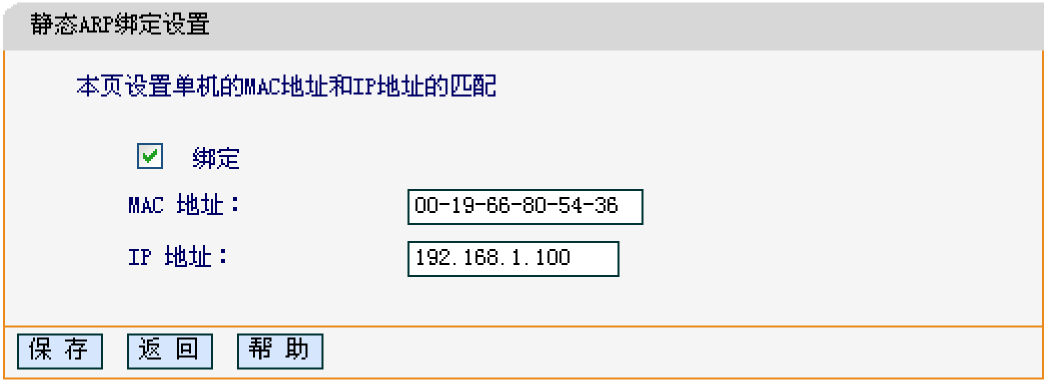


图 4-46 添加静态 ARP 绑定条目

第三步：设置完成后，选中“绑定”，并单击**保存**按钮。

4.12.2 ARP映射表

选择菜单**IP与MAC绑定→ARP映射表**，您可以在图 4-47界面中查看ARP绑定条目信息。

图 4-47 ARP 映射表

- 导入：该项用来将指定映射条目添加到静态ARP列表中(见图4-46)。
- 全部导入：该项用来将ARP映射列表中的所有条目添加到静态ARP列表中。
- 刷新：单击该按钮，您可以更新ARP映射列表中的条目信息。

☞ 注意:

1. 在进行导入操作时，如果该条目与ARP静态绑定表中的某条目冲突，则会显示冲突提示，不会添加该条目;
2. 在进行全部导入操作时，如果同样存在冲突条目，则系统会忽略冲突条目，将其它没有冲突的条目添加到ARP静态绑定列表中。

4.13 动态DNS

选择菜单**动态DNS**，你可以在图 4-48界面中进行相应的功能设置。

动态DNS又名DDNS，它的主要功能是实现固定域名到动态IP地址之间的解析。对于使用动态IP地址的用户，在每次上网得到新的IP地址后，安装在主机上的动态域名软件就会将该IP地址发送到由DDNS服务商提供的动态域名解析服务器，并更新域名解析数据库。当Internet上的其他用户需要访问这个域名的时候，动态域名解析服务器就会返回正确的IP地址。这样，大多数不使用固定IP地址的用户，也可以通过动态域名解析服务经济、高效地构建自身的网络系统。

本路由器提供的DDNS服务为花生壳DDNS，该DDNS的服务提供者是www.oray.net。在图 4-48界面中注册成功后，可以用注册的用户名和密码登录到DDNS服务器上。当连接状态显示成功之后，互联网上的其它主机就可以通过域名的方式访问您的路由器或虚拟服务器了。

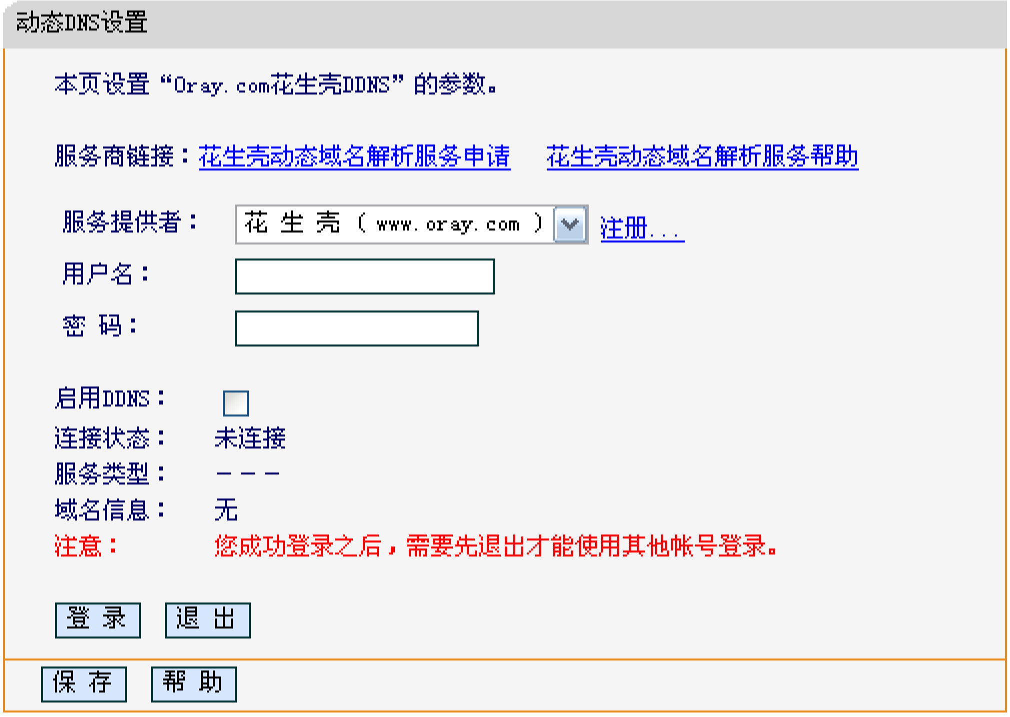


图 4-48 花生壳 DDNS 设置

- 服务商链接：如果您还未在DDNS上注册，请选择该选项进行注册。
- 服务提供者：该项是提供DDNS的服务器。
- 用户名、密码：请正确填写在DDNS上注册的用户名和密码。
- 启用DDNS：该项用来启用花生壳DDNS服务。
- 连接状态：当前与DDNS服务器的连接状态。
- 服务类型：当您成功登录后，该项会显示您注册时帐号所对应的服务类型。
- 域名信息：当前从DDNS服务器获得的域名服务列表。
- 登录/退出：点击该按钮，您可以登录/退出DDNS服务。

4.14 系统工具

选择菜单**系统工具**，您可看到：

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.14.1 时间设置

选择菜单**系统工具→时间设置**，您可以在图 4-49界面中设置路由器的系统时间。您可以选择手动设置时间也可以选择从互联网上获取标准的GMT时间。

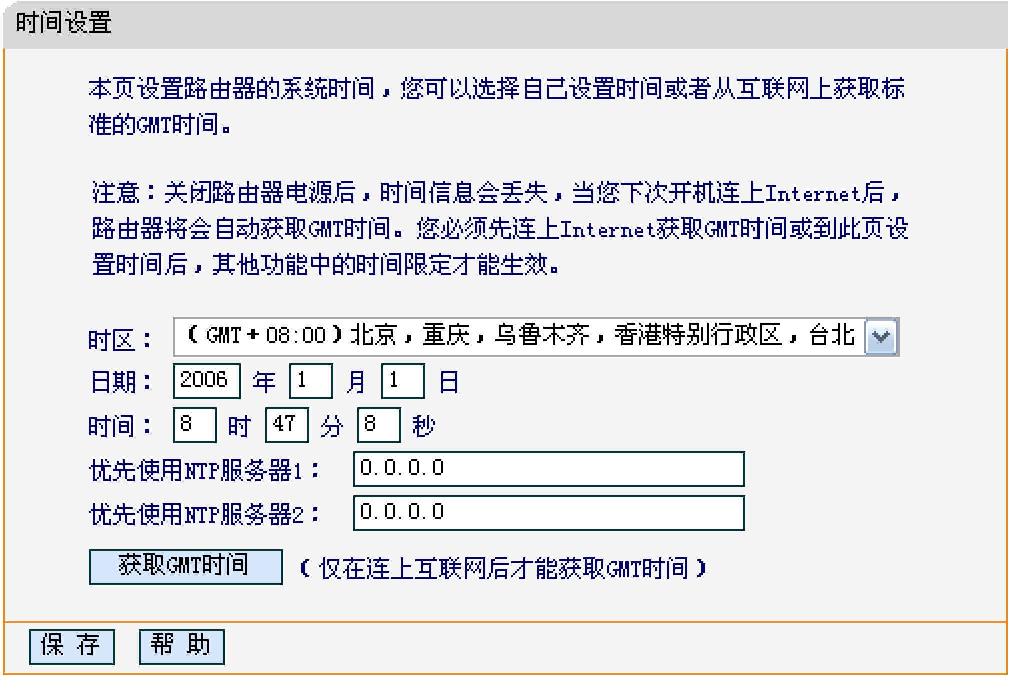


图 4-49 时间设置

- 优先使用NTP Server: 该项用来设置NTP Server的IP地址(最多可以输入两个)。NTP Server是网络时间服务器，用于互联网上的计算机时间同步。该路由器中内置了一些常用的NTP Server地址，一旦与Internet连接后，路由器可以自动获取系统时间。但是，若此处设置了该项，则当路由器获取GMT时间时，将优先从已设置的时间服务器上获取。

时间设置步骤:

手动设置时间: 首先请选择您所在的时区，然后在日期和时间栏内填入相应值，最后单击**保存**按钮即可完成系统时间的设置。

获取GMT时间: 首先请连接互联网，然后选择您所在的时区，最后单击**获取GMT时间**按钮即可从互联网上获取标准的GMT时间。

☞ 注意:

1. 关闭路由器电源后，时间信息会丢失，只有当您下次开机连上Internet后，路由器才会自动获取GMT时间。
2. 您必须先连上Internet获取GMT时间或在此页手动设置系统时间后，路由器其他功能(如防火墙)中的时间限定才能生效。
3. 当选择手动设置时间时，若要查看当前的系统时间，请刷新时间设置页面。

4.14.2 诊断工具

选择菜单**系统工具→诊断工具**，您可以在图 4-50界面中通过使用Ping或Tracert功能来测试路由器和其它主机（包括网络设备）的连接情况。

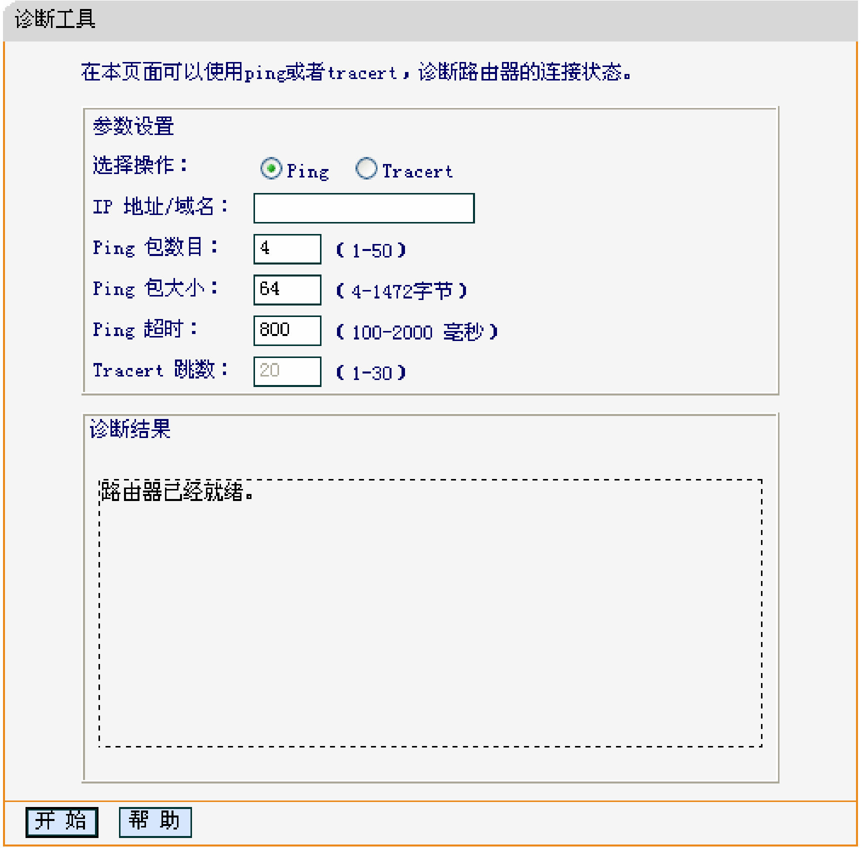


图 4-50 诊断工具

- 选择操作：选择使用Ping或Tracert功能来检测路由器的连接状态。其中Ping功能用来检测路由器和被测主机是否已连通及连接延时等，而Tracert功能用来检测路由器要连通被测主机时需经过的其他路由器的个数。
- IP地址/域名：要检测路由器与之连接状态的设备的IP地址或域名。
- Ping包数目：Ping操作发出的Ping包数目，推荐保持默认值4。
- Ping包大小：Ping操作发出的Ping包的大小，推荐保持默认值64。
- Ping超时：设置Ping操作的超时时间。即超过这个时间没收到回应（Reply）时，认为Ping操作失败。
- Tracert跳数：设置Tracert的跳数，即允许检测的本路由器和被测主机之间路由器数目的上限。

填好相关参数后单击**开始**按钮，路由器就开始进行相应的Ping或Tracert测试了，并显示测试结果。

图4-51是路由器与域名为www.baidu.com的主机正常连接时使用Ping功能诊断的结果，图4-52是路由器与域名为www.baidu.com的主机没有连通时使用Ping功能诊断的结果。

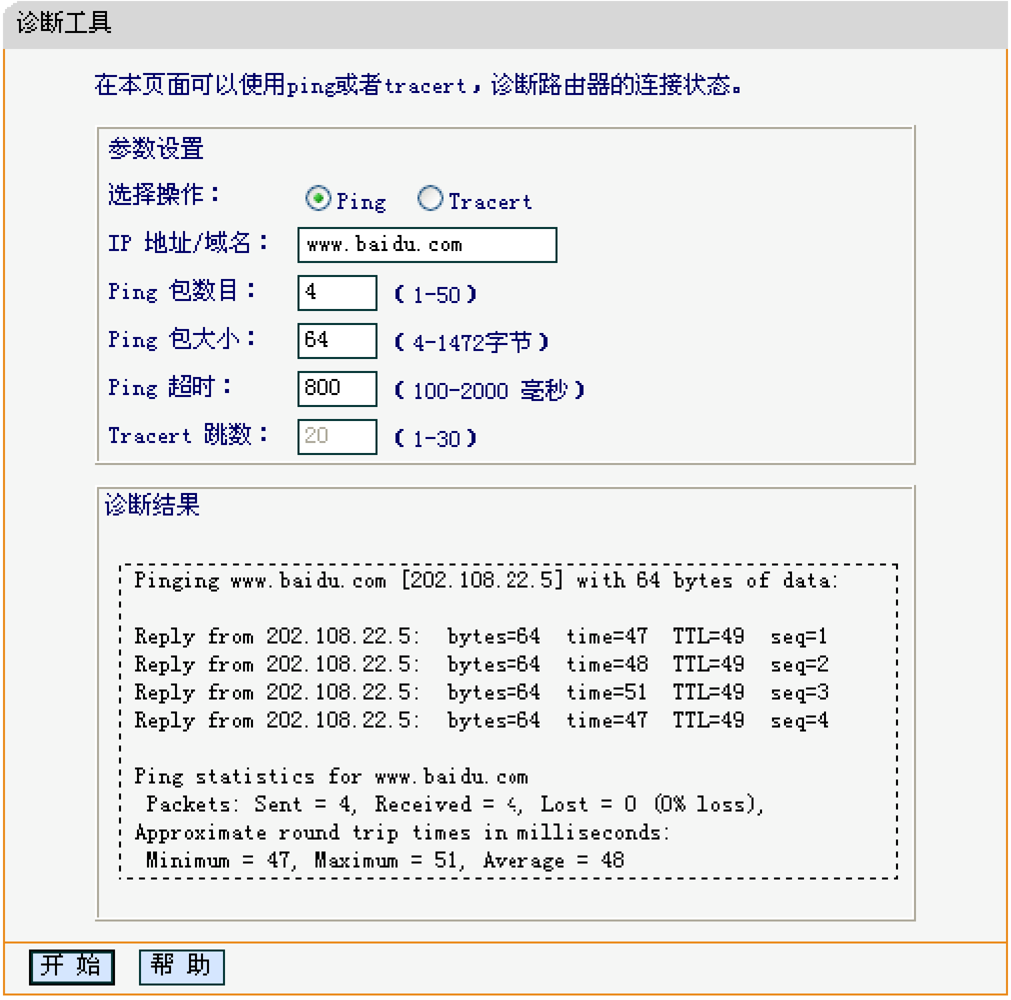


图 4-51 Ping 诊断结果—成功

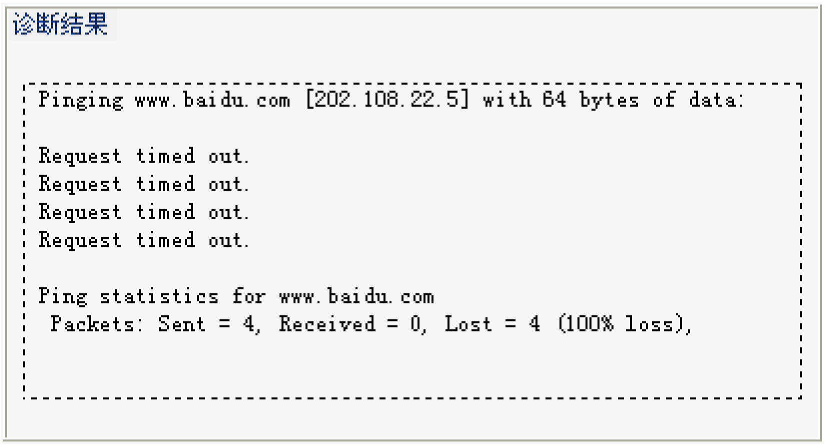


图 4-52 Ping 诊断结果—失败

图 4-53是路由器与IP地址为 10.145.206.66 的主机正常连接时使用Tracert功能诊断的结果，图 4-54是路由器与IP地址为 10.145.206.66 的主机没有连通时使用Tracert功能诊断的结果。

图 4-53 Tracert 诊断结果—成功

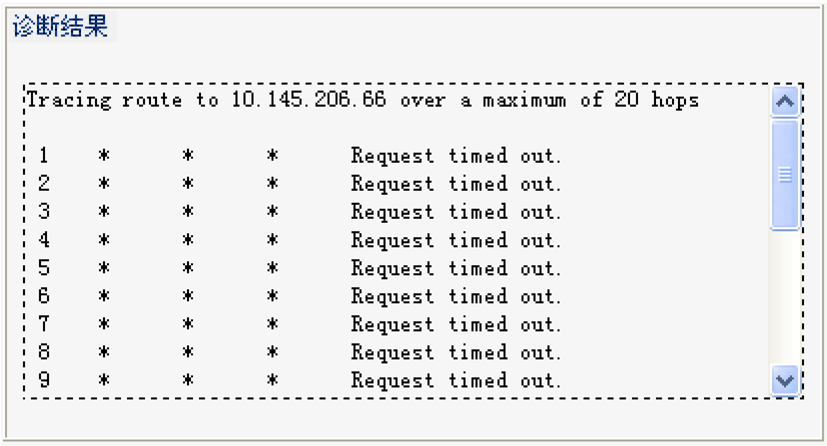


图 4-54 Tracert 诊断结果—失败

4.14.3 软件升级

选择菜单**系统工具→软件升级**，您可以在图 4-55界面中升级本路由器的软件版本。

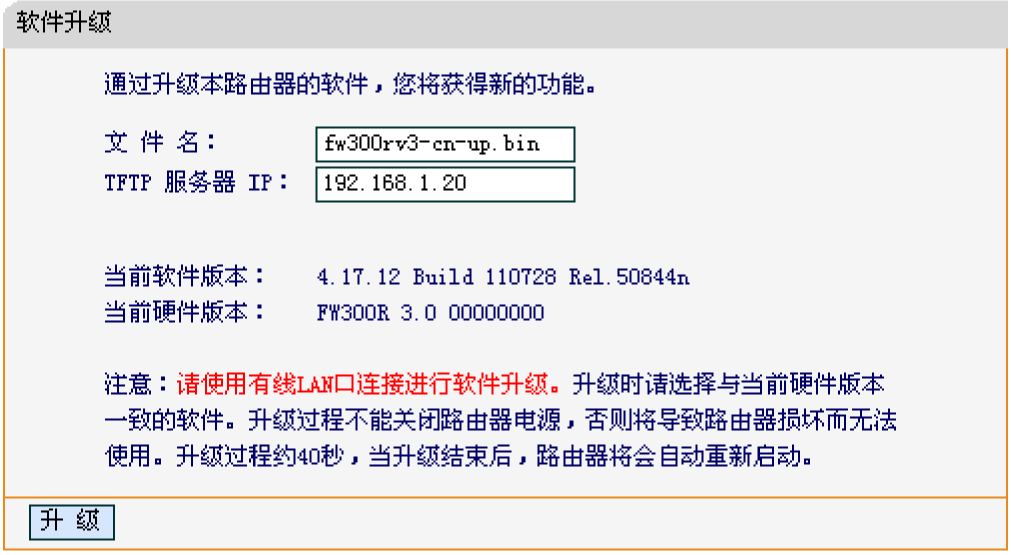


图 4-55 软件升级

软件升级步骤:

第一步：登录本公司的网站(http://www.fastcom.com.cn)，下载最新版本的软件。

第二步：关闭系统防火墙，包括系统自带的防火墙以及您另外安装的防火墙软件。

第三步：双击打开升级包中的 Tftpd32.exe 文件，并确保在整个升级过程中该软件始终处于开启的状态。

第四步：在图 4-55界面的“文件名”栏内填入已下载升级软件的文件名，如“fw300rv3-cn-up.bin”。

第五步：单击**升级**进行软件升级。

☞ 注意:

1. 升级时请选择与当前硬件版本一致的软件。升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。当升级结束后，路由器将会自动重启。
2. 软件升级后，路由器可能会恢复到出厂默认设置。

4.14.4 恢复出厂设置

选择菜单**系统工具→恢复出厂设置**，您可以将路由器的所有设置恢复到出厂时的默认状态。恢复出厂设置后，路由器将自动重启，如图 4-56。

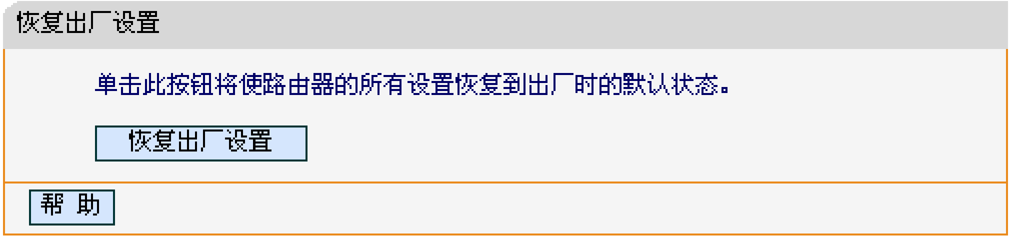


图 4-56 恢复出厂设置

单击**恢复出厂设置**按钮，路由器的所有设置将恢复到出厂时的默认状态。其中：

- 默认的用户名：admin

- 默认的密码：admin
- 默认的IP地址：192.168.1.1
- 默认的子网掩码：255.255.255.0

4.14.5 备份和载入配置

选择菜单**系统工具→备份和载入配置**，您可以在图 4-57中备份或载入路由器配置文件。

配置备份功能可以将路由器的设置以文件形式保存到电脑中，以备下次使用；在升级路由器软件或在载入新的配置文件前备份路由器的原有配置，可以有效防止升级软件或载入新配置文件过程中丢失原有配置的问题。

配置载入功能则可以将先前保存的或已编辑好的配置文件重新载入。如果需要为多台路由器配置相同的设置，则可以先配置一台路由器，保存其配置文件后，再将其载入到其它的路由器中，这样可以有效节省配置时间。

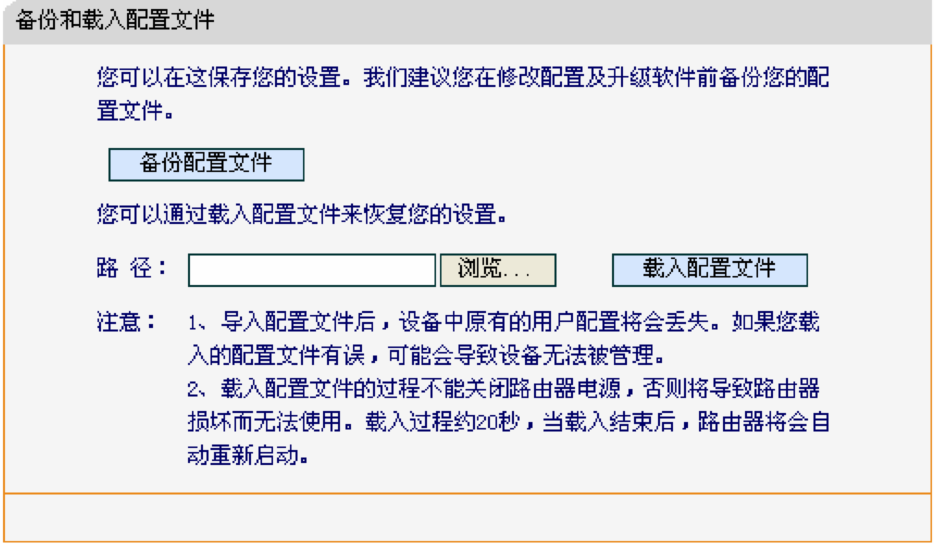


图 4-57 配置文件备份与载入

例1： 如果您希望备份现有路由器的配置文件到C:\Router\backup，您可以按照如下步骤操作。

第一步：在图 4-57界面中点击**备份配置文件**。

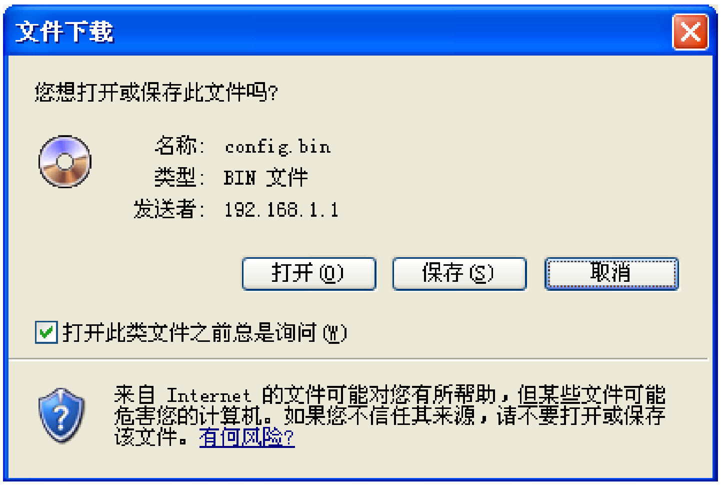


图 4-58 备份配置文件-文件下载

第二步：在图 4-58界面中点击**保存**按钮。

第三步：在图 4-59界面中选择文件存放路径"C:\Router\backup"，然后点击**保存**按钮即可完成文件备份。

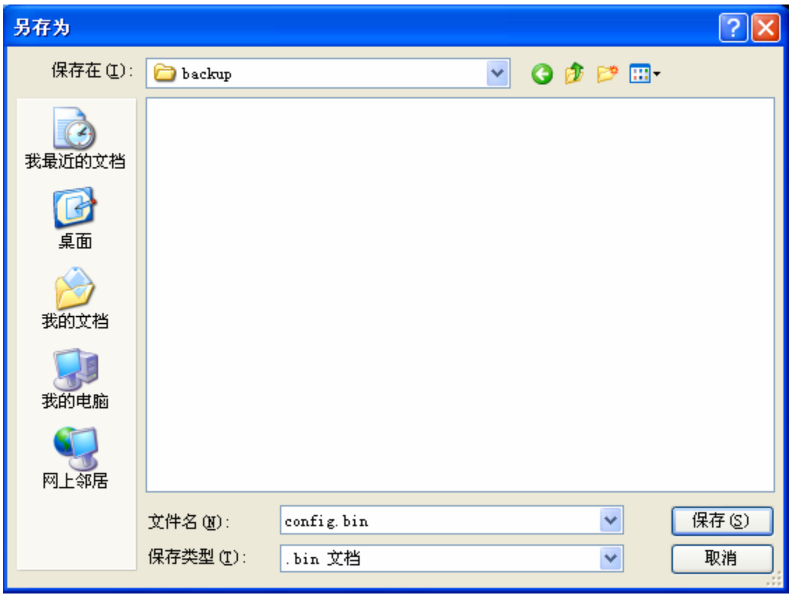


图 4-59 备份配置文件-选择文件存放路径

例2: 如果您希望将C:\Router\backup目录下的config.bin文件载入到路由器中，您可以按照如下步骤操作。

第一步：在图 4-57界面中输入文件的全路径"C:\Router\backup\config.bin"；此处也可以单击**浏览**按钮来选定该文件。

第二步：在图 4-57界面中点击**载入配置文件**按钮。

☞ 注意:

1. 载入配置文件后，设备中原有的配置信息将会丢失，所以在导入配置文件前请先备份配置。如果您载入的配置文件有误，可重新载入先前备份的文件。
2. 配置文件载入的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重新启动。如果载入有错，请根据提示信息自己选择是否保存配置，最好重启路由器。

4.14.6 重启路由器

选择菜单**系统工具→重启路由器**，您可以将路由器重新启动，如图 4-60。

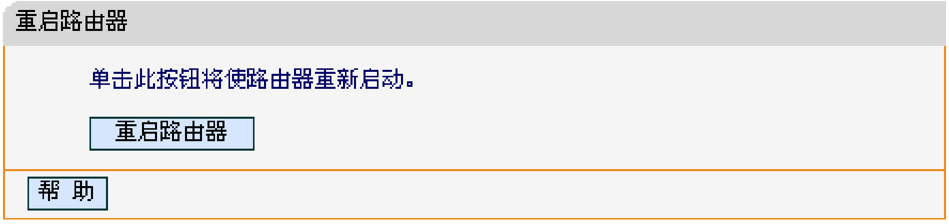


图 4-60 重启路由器

4.14.7 修改登录口令

选择菜单**系统工具→修改登录口令**，您可以在图 4-61界面中修改登录路由器管理界面的用户名和密码。修改时，需要先输入原用户名和原口令，然后再输入新用户名和新口令，如果您原来的用户名和口令输入无误的话，单击**保存**按钮即可成功修改用户名和口令。

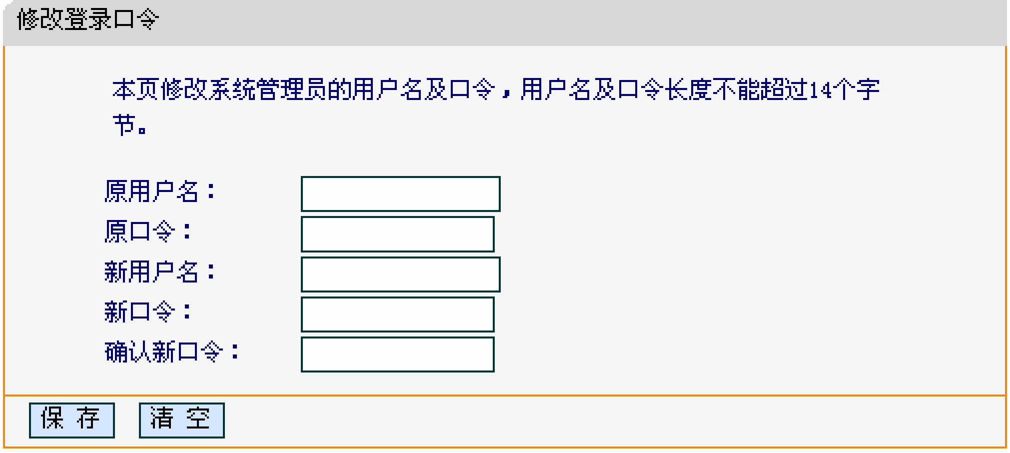


图 4-61 修改登录口令

☞ 注意:

出于安全考虑，我们强烈推荐您更改初始系统管理员的用户名及密码。如果您忘了系统密码，请将路由器恢复到出厂设置(如何恢复请参考2.2 复位)。

4.14.8 系统日志

选择菜单**系统工具→系统日志**，可以在下图 4-62中查看路由器的日志信息。该界面记录了路由器的系统日志，可以通过查询日志了解网络情况和快速定位设备故障。

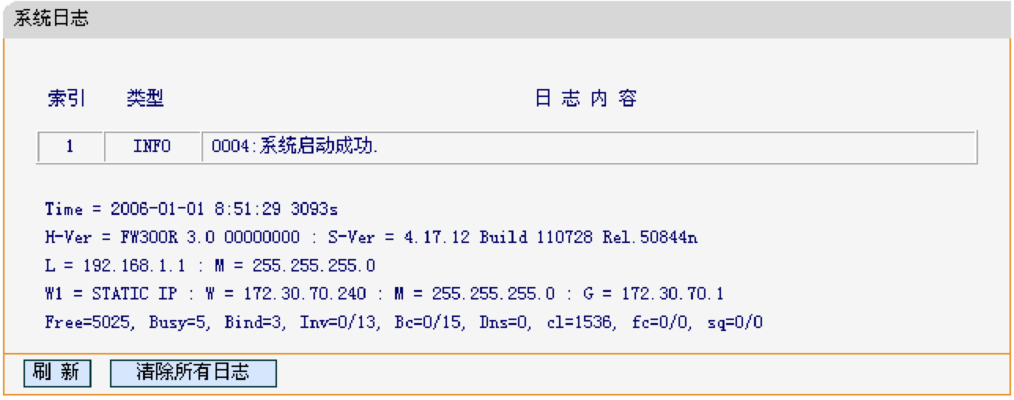


图 4-62 系统日志

- 刷新：点击此按钮，路由器将刷新页面，显示最新的日志列表。
- 清除所有日志：点击此按钮，路由器中的日志将被永久删除。

4.14.9 流量统计

选择菜单**系统工具→流量统计**，您可以在图 4-63中查看路由器的流量信息。单击**刷新**按钮，您可以更新流量统计表；单击**重置**按钮，您可以重新设置统计粒度；单击**删除**按钮，您可以删除指定的流量统计信息。

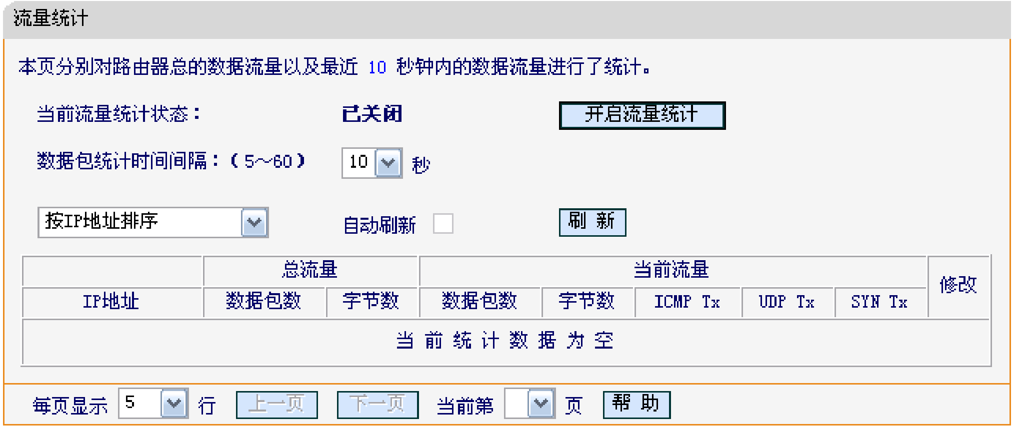


图 4-63 流量统计

- 数据包统计时间间隔：该数值决定了统计路由器当前流量的时间间隔。
- IP地址：被统计主机的IP地址，此处也会显示该主机的MAC地址。
- 总流量：该项分别用数据包个数和字节数来统计路由器接收和发送数据的总流量。
- 当前流量：该项显示在不同的统计单位下，路由器在当前10秒钟内接收和发送不同数据的总流量。

☞ 注意:

若要查看路由器的流量信息，必须先开启路由器的流量统计功能。如无需流量统计，可以关闭该功能，这样可以提高路由器的数据处理能力。

附录A　FAQ

1、 ADSL 用户如何设置上网？

1) 首先，将ADSL modem设置为桥模式(RFC 1483桥模式)。
2) 用网线将路由器的WAN口与ADSL modem相连，电话线连ADSL modem的Line口。
3) 进入管理界面，选择菜单网络参数下的WAN口设置，在右边主窗口中，“WAN口连接类型”选择“PPPoE”，输入“上网账号”及“上网口令”，点击连接按钮即可。
4) 如果是包月上网的用户，可以选择“自动连接”的连接模式；如果是非包月用户，可以选择“按需连接”或者“手动连接”，并且输入自动断线等待时间，防止忘记断线而浪费上网时间。

2、 如何获取正确的DNS服务器地址？

1) 咨询您的网络服务商(ISP)，获取DNS参数；
2) 在操作了路由器成功拨号后，登陆到路由器的管理界面，选择菜单运行状态，然后便可查看DNS参数并记录。

3、 怎样使用NetMeeting聊天？

1) 如果是主动发起NetMeeting连接，则不需要任何配置，直接在NetMeeting界面中输入对方的IP地址，即可进行NetMeeting呼叫。
2) 如果希望能接收对方的NetMeeting呼叫，则需要设置虚拟服务器或DMZ主机，并保证H323 ALG处于启用状态。假设本地主机192.168.1.102希望接收对方的NetMeeting呼叫。
3) 若采用虚拟服务器来实现，设置方法为：进入管理界面，选择菜单**转发规则→虚拟服务器**，点击**添加新条目**按钮，然后在随后的界面中设置“服务端口号”为“1720”，这是NetMeeting的连接端口，然后在“IP地址”栏内填入计算机的IP地址(假设IP地址是192.168.1.102)，再在状态栏选择**生效**，点击**保存**按钮即可。如图1中第三条虚拟服务器条目。

ID	服务端口	IP地址	协议	状态	编辑
1	21	192.168.1.100	TCP	生效	编辑 删除
2	80	192.168.1.101	ALL	生效	编辑 删除
3	1720	192.168.1.102	ALL	生效	编辑 删除

图 1

4) 若采用DMZ主机来实现，设置方法为：进入管理界面，选择菜单**转发规则→DMZ主机**，在“DMZ主机IP地址”栏填入您计算机的IP地址(IP地址是192.168.1.102)，再选中**启用**复选框，点击**保存**按钮即可。如图2。

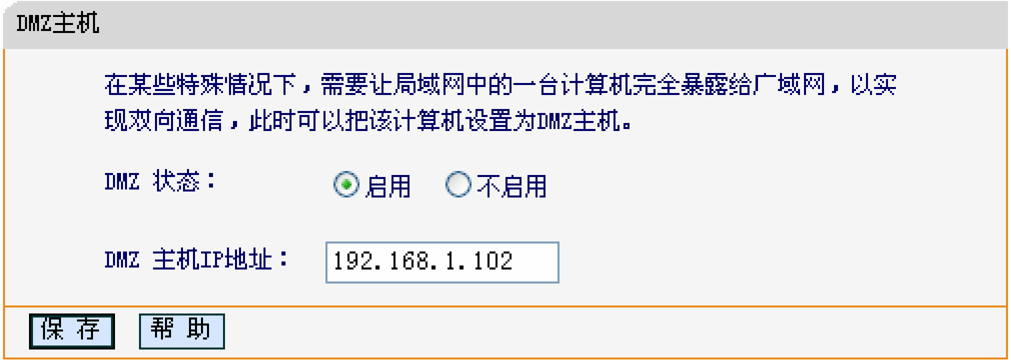


图 2

5) 启用H323 ALG：进入管理界面，选择菜单**安全功能→安全设置**，在“应用层网关（ALG）”中设置“H323 ALG”为启用并保存，如图3。

图 3

4、 怎样在局域网构建Web服务器？

1) 若要在局域网构建其它服务器，只需要参照问题3的第三点设置虚拟服务器即可。

2) 若要构建Web服务器，如果Web的服务端口与路由器Web管理界面的缺省端口相同，都是80时，就会引起冲突。这里的解决办法是更改路由器Web管理界面的端口。具体操作如下：

   登录路由器管理界面，选择菜单**系统工具→远端WEB管理**，在“WEB管理端口”栏输入80以外的值，如88。然后点击**保存**并重启路由器。如图4。

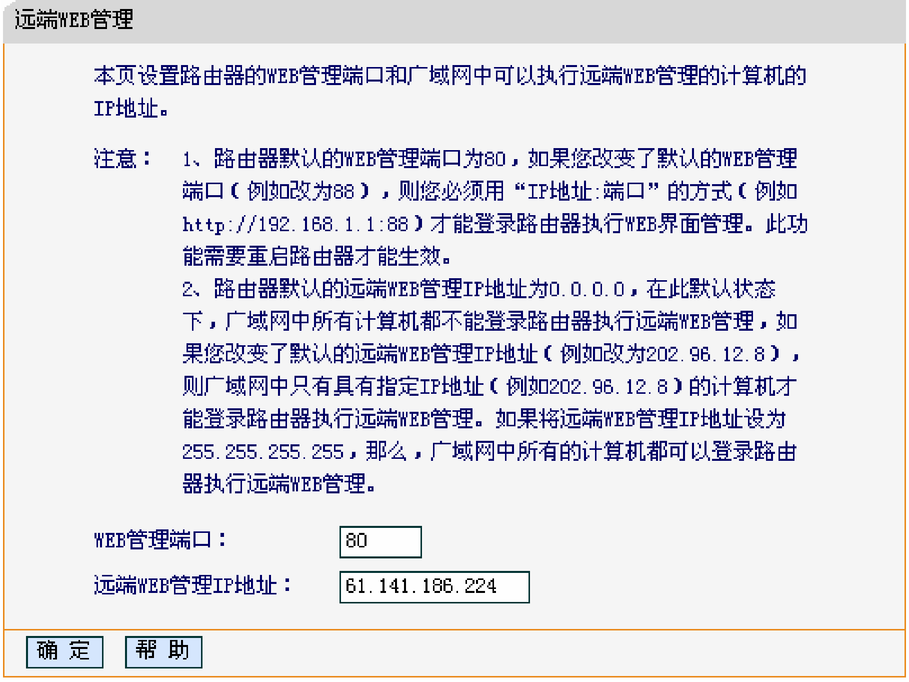


图 4

☞ **注意:**

若要再次登录路由器管理界面，需要在浏览器的地址栏输入路由器WAN口的IP地址和管理端口号才能进行，输入形式为：http://61.141.186.224:88(假设路由器WAN口的IP地址是61.141.186.224)。

3) 登录路由器管理界面，选择菜单**转发规则→虚拟服务器**，点击**添加新条目**按钮，在随后的界面中设置服务端口为“80”，这是Web服务器的连接端口；然后在IP地址栏填入Web服务器的IP地址(假设你指定的Web服务器的IP地址是192.168.1.101)；最后在状态栏选择**启用**并点击**保存**按钮即可。如图5中虚拟服务器中的第二条：

图 5

5、 无线信号受哪些因素的影响？

1) 家庭的空间都比较拥挤，空间不够开阔，其中房间中的墙壁是最主要的障碍物。由于无线局域网采用的是无线微波频段。微波的最大特点就是近乎直线传播，绕射能力非常弱，因此身处在障碍物后面的无线接收设备会接到很微弱的信号，或没有收到信号。

2) 物理的障碍物，不仅阻挡微波无线信号，它还能把电磁的能量给吸收掉，生成弱电流泄流掉，因此，无线信号在家庭环境中最大的金属物体的障碍物是内有钢筋网的楼板，这个方向的信号几乎没有穿透的可能。要能穿透，信号也是非常的弱。

3) IEEE 802.11b/ IEEE 802.11g标准的工作频段为2.4GHz，而工业上许多设备也正好工作在这一频段如：微波炉、蓝牙设备、无绳电话、电冰箱等。如果附近有较强的磁场存在，那么无线网络肯定会受到影响。

4) 如果在无线环境中存在多台无线设备还有可能存在频道冲突，无线信号串扰的问题。

5) 距离无线设备及电缆线路100米内的无线电发射塔、电焊机、电车或高压电力变压器等强信号干扰源，也可能会对无线信号或设备产生强干扰。

6) 信号实在室外传播天气情况对无线信号影响也很大，如果是在雷雨天或天气比较阴沉的时候信号衰减比较厉害，而晴天里信号能传输的距离会更远。

6、 如何改善信号传输质量?

1) 为无线路由选择一个最佳的放置地点。这个放置地点的要求如下：一、位置应偏高一些，以便在较高地方向下辐射，减少障碍物的阻拦，尽量减少信号盲区；二、位置地点选择时应使信号尽量少穿越隔墙，最好是房间中的无线客户端能与无线路由之间可视。

2) 修改频道，减少无线串扰。注意：设置自己无线信号发射频道时也要尽量保证离别人无线信号频道5个以上。

3) 减少居家电器干扰，保证信号畅通无阻。放置无线路由时尽量远离上述设备。

4) 如果无线路由天线是可拆卸的，可以通过更换天线达到增强无线信号的目的。

附录B IE浏览器设置

1. 打开 IE 浏览器，选择菜单工具→**Internet** 选项，如图 6 示。

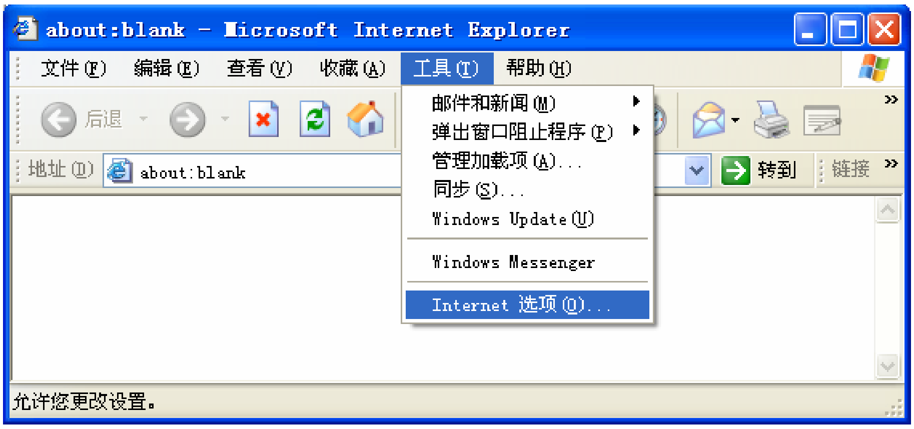


图 6

2. 在 Internet 选项界面中选择**连接**，将“拨号和虚拟专用网络设置”中的设置内容全部删除（该内容为空），如图 7 示。

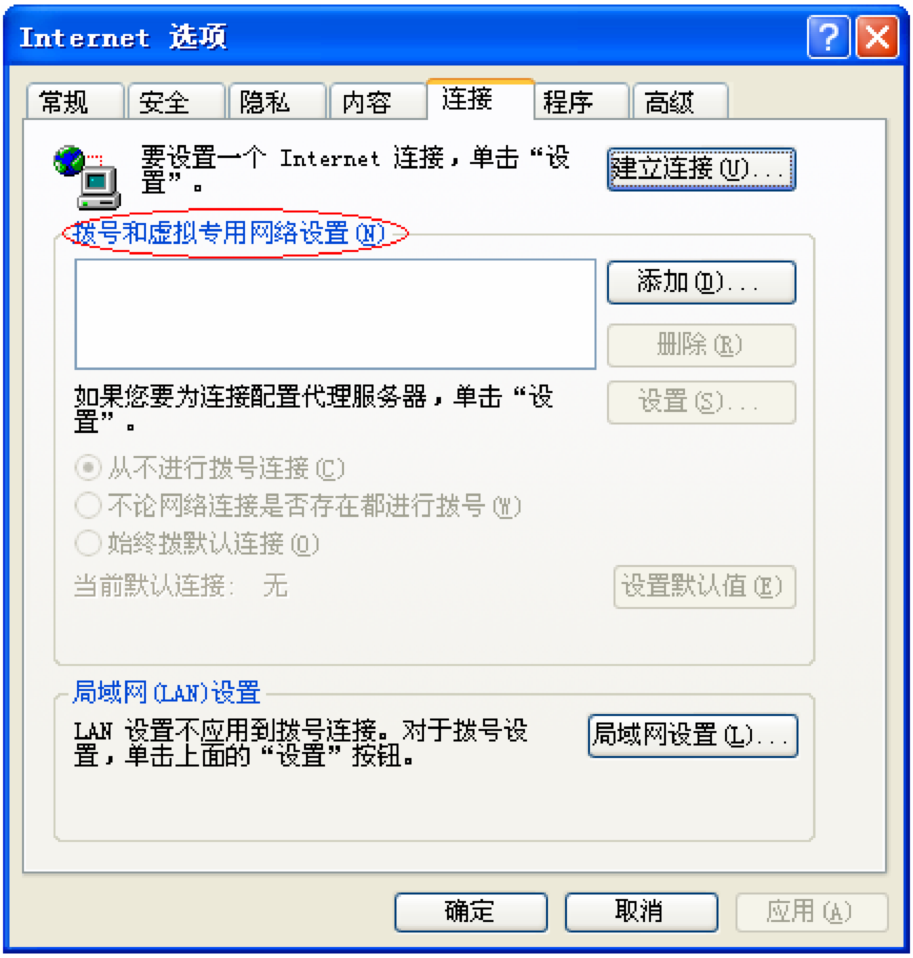


图 7

3. 点击**局域网设置**按钮，按照图 8 界面所示进行配置。之后单击**确定**按钮返回。

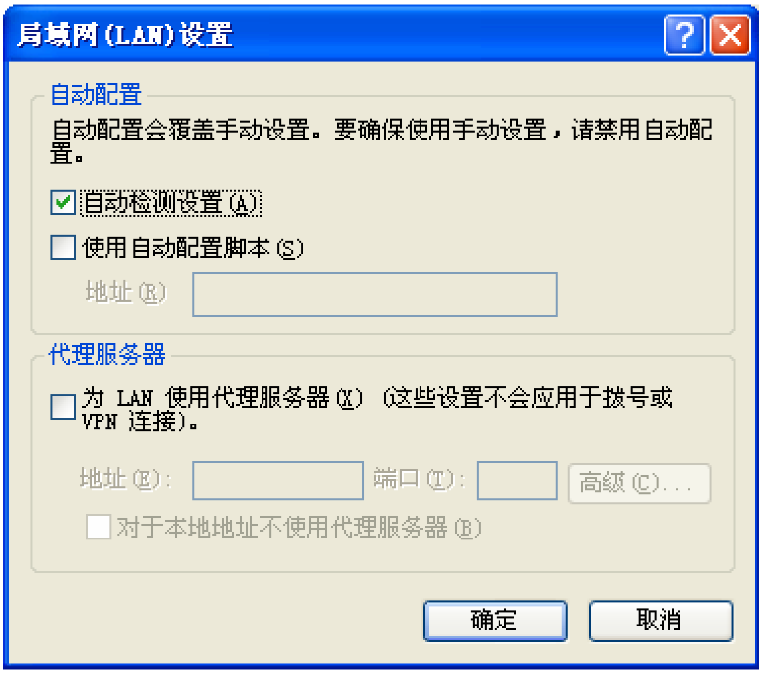


图 8

4. 回到 IE 浏览器界面，选择菜单**文件**，将下拉菜单中的**脱机操作**取消(单击该项将前面的√去掉)，若该项没有启用，则不用设置。如图 9 示。

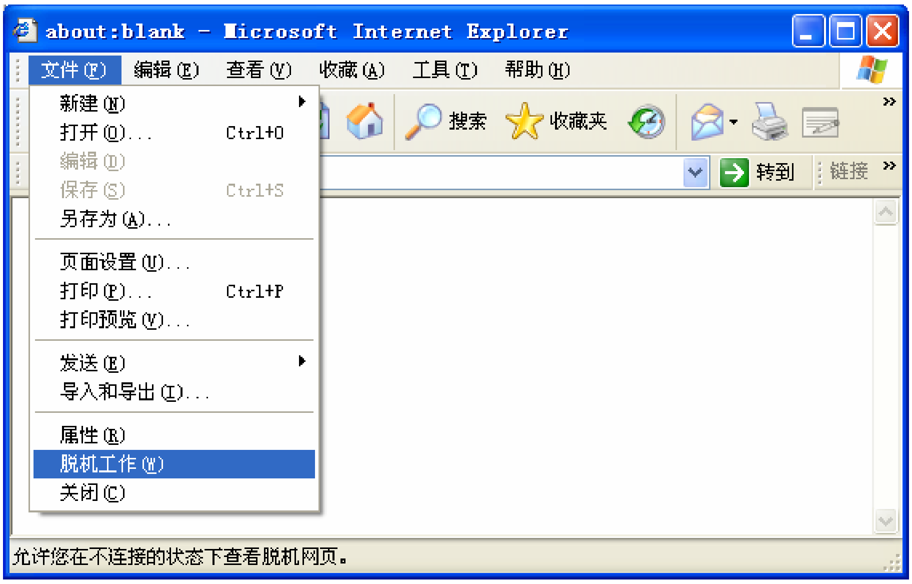


图 9

附录C　规格参数

支持的标准和协议		IEEE 802.11b、IEEE 802.11g、IEEE 802.11n、IEEE 802.3、IEEE 802.3u、IEEE 802.3x、IEEE 802.14X、CSMA/CA、CSMA/CD、TCP/IP、DHCP、ICMP、NAT、PPPoE
端口	LAN口	4个10/100M自适应RJ45端口(Auto MDI/MDIX)
	WAN口	1个10/100M自适应RJ45端口(Auto MDI/MDIX)
无线参数	频率范围	2.4～2.4835GHz
	传输速率	11b：1/2/5.5/11Mbps 11g：6/9/12/18/24/36/48/54Mbps 11n：最高可达300Mbps
	工作信道数	13
	展频技术	DSSS（直接序列展频）
	数据调制方式	11b：CCK,QPSK,BPSK 11g：OFDM 11n：QPSK,BPSK,16-QAM,64-QAM
	介质接入协议	CSMA/CA with ACK
	数据加密	WPA/WPA2；64/128/152-WEP；TKIP/AES
	传输功率	20dBm（最大值）
	天线数目	2根
	天线类型	偶极子全向天线
网络介质		10Base-T：3类或3类以上UTP
		100Base-TX：5类UTP
LED指示	端口	WAN、1/2/3/4(LAN)(指示各端口的Link/Act状态)
	其它	SYS(系统状态指示灯), WLAN(无线状态指示灯)，WPS（一键安全设定指示灯）
外形尺寸(L x W x H)		160mm×103mm×29mm
使用环境		工作温度：0ºC 到 40ºC
		存储温度：-40ºC 到 70ºC
		工作湿度：10% 到 90% RH不凝结
		存储湿度：5% 到 90% RH不凝结